

We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

5,800

Open access books available

142,000

International authors and editors

180M

Downloads

Our authors are among the

154

Countries delivered to

TOP 1%

most cited scientists

12.2%

Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com



Behavioral Biometrics: Past, Present and Future

Mridula Sharma and Haytham Elmiligi

Abstract

Behavioral biometrics are changing the way users are authenticated to access resources by adding an extra layer of security seamlessly. Behavioral biometric authentication identifies users based on a set of unique behaviors that can be observed when users perform daily activities or interact with smart devices. There are different types of behavioral biometrics that can be used to create unique profiles of users. For example, skill-based behavioral biometrics are common biometrics that is based on the instinctive, unique and stable muscle actions taken by the user. Other types include style-based behavioral biometrics, knowledge-based behavioral biometrics, strategy-based behavioral biometrics, etc. Behavioral biometrics can also be classified based on their use model. Behavioral biometrics can be used for one-time authentication or continuous authentication. One-time authentication occurs only once when a user requests access to a resource. Continuous authentication is a method of confirming the user's identity in real-time while they are using the service. This chapter discusses the different types of behavioral biometrics and explores the various classifications of behavioral biometrics-based on their use models. The chapter highlights the most trending research directions in behavioral biometrics authentication and presents examples of current commercial solutions that are based on behavioral biometrics.

Keywords: behavioral biometrics, gait, mouse dynamics, keystroke dynamics

1. Introduction

Multi-factor authentication is a promising authentication method, in which the user is required to provide two or more verification factors to gain access to a service or a resource. Multi-factor authentication could use One time Passwords (OTPs), physical biometrics such as face-recognition or finger-prints, etc. Although passwords have been used regularly for authenticating users for years, they are losing their popularity as passwords can be cracked or stolen quite easily. Biometric security was introduced as a better solution to verify individuals based on their unique characteristics [1]. Physical biometrics, such as fingerprints, face recognition and iris scanning, are currently being used extensively in many applications to secure access to servers and services. However, they are mainly used to perform static authentication to grant access to authorized individuals. Physical biometrics are not commonly used to constantly authenticate users while they are using the service.

With the escalating cybercrimes, static authorization fails to keep systems secure. Session hijacking and man-in-the-middle attacks are just two examples of possible threats that can have significant impacts on systems and networks, even if static authentication was deployed. Therefore, security experts are currently considering the implementation of dynamic, continuous authentication in a wide range of applications. Continuous authentication can be done using behavioral biometrics (BB), which is one of the most promising solutions to this problem. Also known as *behaviometrics*, it is the future of user authentication as it provides a secure, seamless, and hassle-free digital experience. Behavioral biometric authentication systems are currently being deployed in banks, government organizations, and other facilities to provide an efficient protection system against cybercrimes [2].

Since behavioral biometrics is a continuous way of authentication, it keeps checking the behavioral patterns of users. Body movements, voice modulations, typing style and speed, mouse movement styles, and behavior are some of the behavioral biometrics which are known to have uniqueness in it. The behavioral biometrics are primarily based on either the way human-computer interactions take place or the measurements of the body parts and muscle actions [2]. It focuses on how a user conducts a specific activity rather than focusing on an activity's outcome [3].

1.1 Chapter road-map

This chapter begins with an overview of behavioral biometrics in Section 2, which discusses the different types of behavioral biometrics, their advantages, and their shortcomings. Section 3 provides a survey of the research work on behavioral biometrics in the literature. This includes the latest research trends and directions related to behavioral biometrics. There are also several industrial organizations providing commercial platforms that support behavioral biometrics authentication. Section 4 provides a review of those companies and their products. Section 5 presents case studies of various application domains where behavioral biometrics is used for security authentication. Finally, we draw our conclusion in Section 6.

2. Behavioral biometrics: what and why?

With the increasing level of fraud and unauthorized intrusions in various areas of life, especially in banking; the need of multi-factor authentication was significant. Companies and service providers started enforcing multi-factor authentication as a new security requirements to maintain access to services or resources. Biometrics are currently used in many applications as the second level of authentication, along with passwords, for authorizing or even identifying users.

2.1 Behavioral biometrics vs. physical biometrics

There are two main categories of biometrics that are currently being used. These two categories are physical and behavioral. Physical (physiological) biometrics depends on the measurements of a specific individual's features for identity verification/authentication. This includes face geometry, fingerprints, certain parts of the eye, vein patterns, and other corporal traits. To put it simply, physical biometrics replace "things that you know" (passwords and PINs) with "things that you are" [4]. Other examples include DNA, ear, footprint, palm print, retinal, etc.

On the other hand, behavioral biometrics is the measurement and analysis of human-specific behavioral traits based on human movement or their interaction with the computer parts, such as mouse, keyboard or handheld devices like ipads, or phones.

Physical biometrics are commonly used for one-time authentication, whereas, for dynamic authentication, behavioral biometrics can be more effective. Behavioral biometrics deployment can be divided into four distinct types of applications: continuous authentication, risk-based authentication, insider threat detection, and fraud detection and prevention [3, 5]. Behavioral biometric authorization integrates three main fields: human behavioral pattern analysis, smart sensors technologies, and machine learning models.

The biometric types are shown in **Figure 1**.

2.2 Advantages of behavioral biometrics

There are many advantages of behavioral biometrics over physical biometrics. The following points highlight these advantages [5–7].

- **Continuous collection and authorization**—Behavioral biometrics enable constant monitoring of users. This helps to ensure that only the authorized user is the one who is using the system, even after the initial identity check has been done.
- **Non-obtrusive collection**—The behavioral data can be collected in a seamless manner without disturbing the normal service usage.
- **No need of special hardware**—The behavioral data may be collected using a standard camera or voice recorders. The video or audio recordings are processed to retrieve the data for authorization afterward.
- **Useful for authorization**—Behavioral biometrics deliver continual user authentication and is a powerful defense. But it is only a complement to one-time

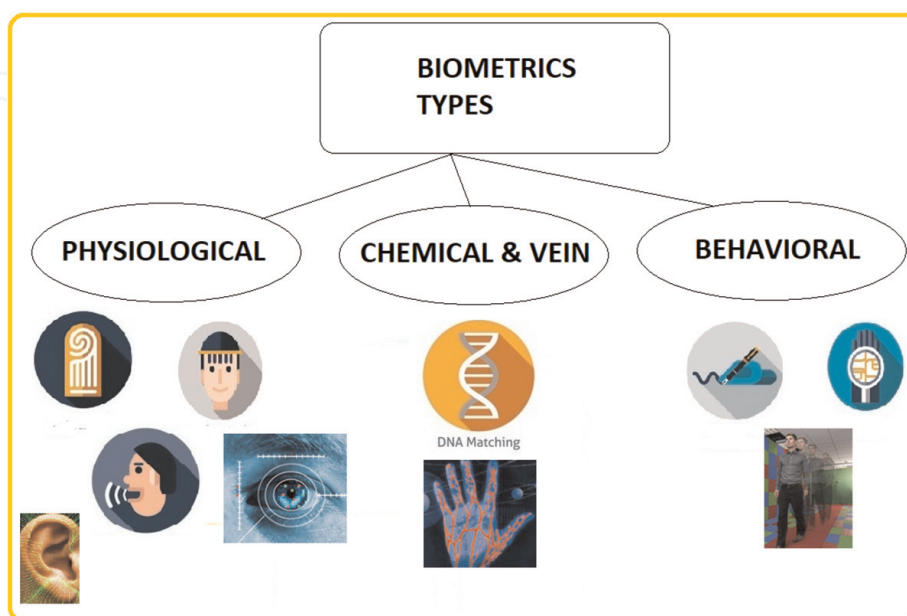


Figure 1.
Types of biometric.

authentication techniques such as passwords, PIN, and other physiological biometrics.

- **Universality**—When applied to a large population, the universality of behavioral biometrics is very low as the degree of difference in behaviors may not be very large. But when used in a specific domain, the actual universality of behavioral biometrics reaches up to 100%, making it highly acceptable.
- **Circumvention**—Behavioral biometrics traits are very difficult to emulate or copy.
- **Unique combination**—Behavioral biometrics is mostly a unique combination of analyzed behavioral characteristics for each real person.
- **Smooth Integration**—Once the behavioral biometrics model is defined, it can be integrated very easily with already existing security systems. For example, the regular video surveillance system can be utilized to implement behavioral biometrics system.
- **High verification accuracy**—In multi-modal identification systems, the behavioral biometrics verification accuracy is proven to be quite high.
- **Acceptability**—Most often, behavioral biometrics are collected without user participation. Therefore, it does have a high degree of acceptability. However, on privacy and ethical grounds, it faces several objections as well.

2.3 Shortcomings of behavioral biometrics

Although behavioral biometrics authentication has high accuracy and acceptance rate, it still has several challenges that hinder the implementation of such systems in a wide range of applications. The following points highlight these challenges.

- **Implementation Cost**—Although, the new hardware is not required, still a framework that can create the dataset for behavioral biometric analysis needs to be built and integrated separately into the existing security systems. The implementation of such a new framework can be costly since it is still in the development stages.
- **Large Data Acquisition**—The integration of behavioral biometrics authentication requires the collection of huge personal data records to profile a user's typical behavior accurately.
- **Adaptation to Behavioral changes**—One of the biggest challenges is the ability to create a classification model that can adapt to behavioral changes. Changes in human behavior can happen for many reasons, such as external factors like weather, tiredness, or even aging. Behavioral biometrics authentication models need to be constantly re-trained to be up to date with the changes in human behavior. People may behave differently when they are in a hurry, tired, drunk or when they are not feeling well. Behavioral biometrics models face many challenges related to the adaptation to behavioral changes.

- **Privacy Issues**—Some users are still reluctant to use behavioral biometrics authentication due to ethical and privacy issues.

2.4 Commonly used behavioral biometrics

Behavioral biometrics systems measure various human actions. These actions can be the result of human skills, such as motor skills, style, preference, knowledge, or strategy [5]. Based on the traits and features used for collecting human behavior, behavioral biometrics can be classified as:

- **Skill-based Behavioral Biometrics**—The behavior is based on the instinctive, unique and stable muscle actions taken by the user. Examples are car driving style, keyboard dynamics, programming style, gaming, etc.
- **Knowledge-based Behavioral Biometrics**—The knowledgeability of the user is recorded as their usual behavior. Examples are biometric sketch, text authorship, etc.
- **Style-based Behavioral Biometrics**—Each user has a unique style that can be used to authorize them. Examples are haptic, gaming, programming, mouse, painting, email behavior, gesture etc.
- **Strategy-based Behavioral Biometrics**—Users may have a specific strategy that they adopt. An example is the gaming technique.
- **Preference-based Behavioral Biometrics**—Based on the user's preference of words, letters, or their belongings. Examples are credit card usage, bank usage, tool usage, language usage etc.
- **Motor-skill-based Behavioral Biometrics**—Based on the muscle-control actions of the users makes it innate, unique, and stable. Examples are blinking, GAIT, handgrip, haptic, lip movement, signature, tapping, voice/speech, etc.

2.5 How does behavioral biometric authentication work?

For the purpose of identification or authorization, behavioral biometrics data is first collected and stored. The data is processed further to prepare a signature profile. Using machine learning classifiers, predictive models are trained, developed, and evaluated. Later, this model is used as a comparison tool, whenever the user uses the application. Using behavioral patterns, the model is used to continuously verify the user's profile throughout their working sessions. The generic architecture of a biometric system consists of five main modules:

- **Data Collection Module:** This module captures the biometric raw data to extract a numerical representation.
- **Feature Engineering Module:** To reduce the extracted numerical representation and optimize the data into required features that need to be stored for the verification and identification purposes.

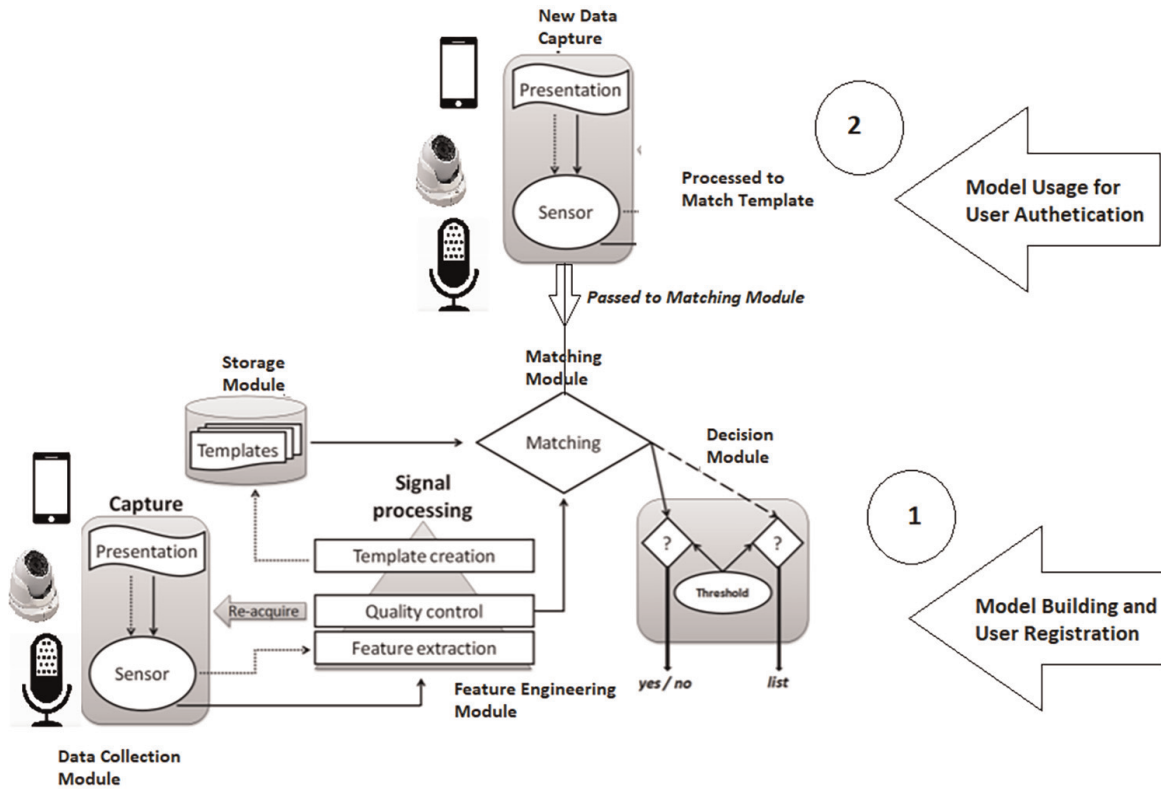


Figure 2.
Behavioral biometric model.

- Storage module: This module stores the individuals’ biometric profiles in the form of dataset.
- Matching module: The module is used to compare the newly extracted biometric profile to one or more previously stored profiles.
- Decision module: This is the verification step to return a value that decides for identification/authorization.

The BB model is shown in **Figure 2**.

3. Behavioral biometrics models in literature

Behavioral biometrics has drawn the attention of both researchers and industry experts. The common areas where behavioral biometrics has played a very important role are user profiling, user modeling, opponent modeling, criminal profiling, jury profiling, etc. [5]. The information/data that may be collected for behavioral analysis may come from several sources like sensors, cameras, keyboard and mouse usage, device, audit logs, signatures or handwriting, programming style, language, smell, etc. [5]. Moreover, physical traits like odor, heartbeat, and even DNA are also being used in some applications. Researchers have also started exploring ECG, brainwaves, and passtoughts to analyze behavioral traits [5].

The most commonly used behavioral biometrics is keystroke dynamics. Keystroke dynamics have been used to authenticate users for years. Keystroke dynamics data can

be collected by typing standard or non-standard passwords. Features extracted from the raw data that represent the typing patterns are used to create a unique profile for each user and to authorize those users later to resources [8–10]. It can also be used to recognize the emotions of a person [11]. To recognize the emotion from typing patterns, users are asked to type a specific sentence. Using feature extraction techniques, predictive models can be trained to classify various emotions. In one study, touch sense was defined and created as an emotion detection model based on typing and swiping patterns of a user with an accuracy rate of 73% [12]. Typing and swiping patterns are used in several applications to detect the emotions of smartphone users [12].

Another example of behavioral biometrics is mouse dynamics, where the recognition of a user profile is done based on the way a user uses his/her mouse on the computer [13–15]. The behavioral profile is created by extracting specific features related to the mouse movements of a user. Mouse and keystroke dynamics are related and complement to each other. The use of the mouse is very important in graphical user interface applications, while the keyboard is commonly used in word processing and command-line applications [16]. Mouse and keystroke dynamics are significantly important in enhancing computer security.

One of the most interesting research directions in behavioral biometrics is GAIT analysis. GAIT analysis is used to authenticate users based on their style or manner of walking [17, 18]. GAIT analysis systems depend mainly on a video camera, that captures images of people walking within its field of view. The images are processed to get appropriate features of users such as joint angles or silhouettes and the values are then compared to the stored gait signatures and profiles of the authorized individuals. One of the main advantages of GAIT analysis is that it is non-intrusive, which means that it does not require cooperation from the individual, and can function at moderate distances from the individual under observation.

Biotouch is another framework based on behavioral biometrics and location for continuous authentication on mobile banking applications [19]. Biotouch uses touch patterns for profiling users while typing and holding the device. This data is then used for predictive model building and authorization.

A new technique in profiling users' behavior is creating users' profiles based on their game playing styles. This technique analyzes the strategies used while playing a game and creates a user profile based on these strategies, as a type of behavioral biometric. These profiles are used later for continuously observing and authorizing the player to the servers [20]. One example of using this new technique is exploring the strategies used while playing the poker game to create behavioral biometric profiles [20]. Once a profile is created, it can be used to authorize the player on the go.

Another interesting approach is using odor as a biometric to identify individuals [21]. In this approach, the tiny quantities of molecules that constantly evaporate and produce the smell, known as odorants, are detected by a special sensor called *e-nose*. *e-nose* is a chemical sensor that can be used to collect unique data about each individual participant. The data can be used to train classification models and to authenticate users [22]. *e-nose* is a rapid, noninvasive, and intelligent online instrument based on the feasibility and effectiveness of odor recognition. Made up of an array of sensors, it is an appropriate pattern recognition system, which is capable of identifying particular smells.

Facial recognition and emotion detection have been used in many applications to classify users. Gabor wavelets is a method to extract features from an image for recognition. For example, analyzing facial images for face recognition by pre-processing or normalizing the face image [23]. As a common rule, the eyes and the

Behavioral Biometrics	Purpose
Keystroke Dynamics	To recognize a person using keystroke dynamics [11].
Keystroke and Mouse Dynamics	Identity theft issues by verifying users based on their keystroke dynamics and mouse activities [26]
Touch and hold a device	Emotion detection from touch interactions during text entry on smartphones [12]
Touch Patterns	continuous authentication on mobile banking applications [19]
Mouse Dynamics	Computer user recognition based on the way a user uses his/her mouse [15]
GAIT	Authorization process based on style or manner of walking [17, 18]
Strategy	Player profile is used to authorize the player on the go [20]
Odor	Human recognition through the odor authentication [21]
Gabor wavelets	To extract features from an image for recognition [23]
Handwriting Biometric	A process of transforming a language represented in its spatial form of graphical marks into its symbolic representation [24]
Speech	Useful for biometric authentication, forensics, security, speech recognition, and speaker diarization [25]

Table 1.
Behavioral biometric research work.

mouth will always be aligned roughly at the same position in same-sized images for face processing. Gabor filters for different scales at different orientations are applied to each facial image for the purpose of creating feature vectors to train machine learning models.

Several researchers considered handwriting biometrics as behavioral biometrics as they are based on actions performed by a specific subject. Handwriting recognition is the task of transforming a language represented in its spatial form of graphical marks into its symbolic representation [24].

Voice recognition is one of the behavioral biometrics that can be used to identify a vocal pattern based on sound variations that are most common in a person's speech. Both speaker identification and speaker verification can be done by capturing important narrow-band speaker characteristics such as pitch and formats [25]. This technique is used for biometric authentication, forensics, security, speech recognition, and speaker diarization.

A brief list of previous studies is given in **Table 1**.

4. Behavioral biometrics solutions in the industry

Not only researchers, but many industry experts are working diligently to improve the applications and performance of behavioral biometric solutions.

4.1 BioCatch

Founded in 2011, BioCatch is working diligently to address next-generation digital identity challenges by focusing on online user behavior. BioCatch has developed several solutions that could improve security in the following use cases: 1) Account

opening protection, 2) Account takeover protection, 3) Social engineering scam detection, 4) PSD2 strong customer authentication, etc. [27]. As per BioCatch, “In our digital world, behavior tells all” [27]. Regardless of an attacker’s chosen mode of operation, user behavior can never be stolen, spoofed, or replicated. BioCatch has developed solutions that can continuously monitor a user’s physical and cognitive digital behaviors. These solutions can be used to analyze thousands of interactions per session and build models to distinguish between genuine and non-genuine users. The solutions are used for several surveillance systems like account opening protection, account takeover protection, advance social engineering, payment scams, proactive mule detection etc.

BioCatch is providing its software products to many leading banks and helping them to prevent identity thefts and other frauds detection and protection. Some major clients for BioCatch are HSBC, American Express, etc. [27].

4.2 Simprints

Simprints works on the motto of “Transforms the way the world fights with poverty”. They are working on building technologies that can be used to identify the person with fingerprints to generate biometric ID for data analysis. The plan is to build a technology that can radically increase transparency and effectiveness in global development, making sure that every vaccine, every dollar, every public good reaches the people who need them the most [28].

4.3 PluriLock

Founded in 2016, Plurilock is working to provide an advanced authentication system using behavioral biometrics [29]. They use the concept of device-based gestures to authenticate users using keystroke dynamics and mouse movements in their two products namely, PLURILOCK AWARE and PLURILOCK DEFEND [29].

- Plurilock Aware—deals with the problem of login credentials, and ends up the frustration of typing passwords and OTP. It provides identity verification by recognizing the typing patterns of the users. It is invisible to the users, not-stealable, and takes care of privacy.
- Plurilock Defend—detects the legit person, while the session is on, using continuous authentication. It also monitors the session activity. Using continuous keystroke and mouse monitoring, the risk is reflected and the system is alarmed.

The AWARE and DEFEND products use patented algorithms to bring continuous authentication to highly-regulated environments like government, critical infrastructure, financial services, and healthcare.

4.4 TypingDNA

Using keystroke dynamics, TypingDNA provides continuous authentication. Founded in 2016, TypingDNA works on recognizing a person’s typing behavior for authorization. The company had launched four products for verification and authentication purposes:

- **VERIFY 2FA**—a 2-factor authentication product, which has an AI agent, which examines and saves the typing pattern of a user for future verification [30]. The second product is authentication API. It uses four different ways to authenticate the user.
- **Login authentication**—when the user logs in for the first time, it will register that typing behavior and will use the created profile to verify the user later. When the user types his login credentials next time, the AI will match it with the first enrollment. If more than 90% of the features match, then the user will be authenticated [31].
- **ActiveLock**—This product is used to restrict the unauthorized access to the company computers using continuous authentication. If any bizarre typing pattern is recognized by the system, it will automatically lock the computer system. Also, if an authorized person forgets to log out of his computer and any unauthorized person tries to access the data, continuous authentication will catch the unusual behavior and will lock the system [32].
- **Focus**—Based on the typing patterns, this application helps users to recognize what mood they are in and what time of the day they are more productive. This application works as a mood tracker. When the user types anything, it examines the typing behavior and analyzes several features. This includes: when the user is actively engaged in typing, for how long he was typing, the typing speed and the typing volume. The tool uses AI to predict the mood of the user [33].

4.5 ThreatMark

The company provides a complete package to prevent current and future digital fraud since 2015 [34]. ThreatMark is working to prepare solutions for banks to fight fraud, from early threat detection, over behavioral biometrics to transaction risk analysis.

- **Anti Fraud Suite (AFS)**—Innovative, feature-rich and modular Fraud Detection Solution for Digital Banking and Payments featuring behavioral profiling, including behavioral biometrics, transaction risk analysis and threat detection in one machine learning-based analytics engine.
- **Clair**—Unique Solution for Online lending, Gaming and other businesses looking to minimize fraud risk and/or credit risk. Clair is using behavioral profiling and biometrics to identify users, predict future business outcomes, fraud and more.

4.6 3DiVi

Founded in 2011, 3DiVi Inc. is an AI technology company focused on the application of deep learning to computer vision [35]. The company is working on developing state-of-the-art API/SDKs that enable smart devices to recognize humans. Their solutions are used by several big companies like Intel, Adidas, LG, Orbbecc etc. The company is working hard to enable human-machine interface (HMI) in IoT, smart home, smart retail, smart car, robotics, and digital identity verticals. The product line has several specialized SDKs.

- NUITRACK SDK—a 3D tracking middleware developed by 3DiVi Inc. This is a solution for skeleton tracking and gesture recognition that enables the capabilities of Natural User Interface (NUI) on Android, Windows, and Linux.
- Interactive Android™ Box—Game with gesture recognition—Ultimate platform to build and sell applications with full body and face interactivity.
- Face SDK—face recognition with a suite of solutions designed to enhance business capabilities, automate tasks, and increase overall community safety.
- SEEMETRIX—Anonymous Face Analytics. This solution can be used to detect gender, age, emotions in a fraction of second

4.7 Zighra

Zighra makes authentication more secure than static MFA and enables passwordless experiences [36]. Their platforms, combine insights from generative behavioral models and biological systems to train faster, dynamically adapt, and accelerate execution compared to AI approaches commonly used today.

The software provides task-based authentication where users are asked to perform a specific action as an authenticator to determine whether the user or a bot is trying to use the device, such as holding the phone and swiping across the screen. It also provides security intelligence, using the unique ways a user types, swipes, and taps.

Transaction risk assessment is done using machine learning and behavioral biometrics to ensure the identity of the user on the device and also provides proof of presence using AI, behavioral biometrics, sensor analytics, and network intelligence together to actively authenticate the identity of the on-device user [36].

They have been awarded an innovation contract to pilot continuous authentication for remote access using patented next generation AI technology by the government of Canada [37].

4.8 VoiSentry

A speaker identification and verification (ID&V) system developed by Aculab, that captures tens of thousands of unique voices and speech characteristics to authorize the user on the go [38]. This solution is an ideal system for voice biometric authentication system in terms of performance and accuracy.

4.9 Cynet

Cynet's user behavior analytics system continuously monitors and profiles the user activity [39]. This profile is later used to define a legitimate behavioral baseline and identify anomalous activity to indicate any compromise in the user accounts. It provides real-time monitoring of all the interactions from the time users initiate by logging in.

4.10 BehavioSec Inc.

The BehavioSec solution provides a continuously learning AI subsystem with pre-weighted machine learning models based on prior analysis, using a hybrid of offline and

online calculations [40]. The company leverages APIs, SDKs, and rich behavioral biometrics insights, that can be used to embed seamless security into the existing systems.

4.11 SecureAuth Inc.

Working toward deploying MFA in a digital world [41]. The initiatives are password authentication, portal and web apps security, RSA migration etc. The products are deployed in several industries like healthcare, retail, energy, financial, and public sectors.

4.12 UnifyId

They are the developers of a passive behavioral authentication platform designed to identify users without any conscious user action [42]. The platform developed

Company Name	Year	Types	Used by
BioCatch [27]	2011	Typing speed, Swipe pattern, mouse clicks	HSBC, Itau, BARCLAYS, nab, American Express, citi VENTURES, 86400 banks, NatWest
Simprints [28]	2012	Wireless Fingerprint scanners	BRAC, Cohesu
Plurilock [29]	2016	Keystroke dynamics, Pointer dynamics	US federal agencies
TypingDNA [31]	2016	Keystroke dynamics	Microsoft Azure, ForgeRock, Optimal IdM, BBVA, Proctoru, Capgemini
ThreatMark [34]	2015	Mouse events, keystroke dynamics, site navigation patterns, interaction with website elements	SLOVENSKÁ SPORITELŇA(Bank), SBERBANK
DiVi [35]	2011	Facial Recognition, Skeleton tracking	Intel, Adidas, LG, Orbbec
Zighra [36]	2010	Task-based authentication using behaviors such as holding the phone and swiping across the screen	Government of Canada innovation Fund
VoiSentry [38]	2018	Speaker identification and verification system	ForgeRock, University of York, MyForce
Cynet [39]	2018	Behavior analytic System to continuous monitoring	Darktrace, Microsoft Azure, Vectra Networks
BehaioSec Inc. [40]	2010	The API can turn behavior into actionable intelligence with just a few lines of code	IDG, Gartner, Goode Intelligence
SecureAuth Inc. [41]	2015	Identity Security Without Compromise	Xerox, Michaels, Unisys
Unify Id	2015	Passive behavioral authentication platform designed to identify users without any conscious user action	US banks
SecureTouch Inc.	2014	Deliver continuous authentication technologies to strengthen security and reduce fraud	Zaraz, Neon Media, TimeRack

Table 2.
Behavioral biometric commercial organizations.

utilizes sensor fusion with machine learning to provide enhanced accuracy while improving the user experience. This helps in authentication both in application and in the physical world.

4.13 SecureTouch Inc.

A pioneer in the field of behavioral biometrics for mobile. They work to deliver continuous authentication technologies to strengthen security and reduce fraud while improving customers' digital experience [43]. Their systems seamlessly collect and analyze a dynamic set of over 100 different behavioral parameters like keyboard-typing, scroll-velocity, touchpressure, and finger size to automatically create a unique user behavioral profile, which can be used for authorization later.

Table 2 provides a summary of the companies working on behavioral biometrics technology.

5. Continuous authentication use cases using behavioral biometrics

With the estimation of the growing behavioral biometrics market which is expected to reach \$4.62 USD billion by 2027, it has almost grown in every area of usage [44]. In this section, we present some common applications where behavioral biometrics is used very extensively.

- ***Student authentication using typing biometrics***—the need is to have continuous identity and authorship assurance throughout the learning activities within the existing learning space for learning and assessment [45]. Behavioral biometrics is used to make a model that can be applied to measure the degree of learner collaboration with peers and also define and verify the interaction with the course content. Also helpful in validating authorship of the academic artifacts.
- ***Proliferation in desktop and workplace computing***—Same keyboard, mouse, and touch patterns together can help in authorization and controls on the desktops and workplace computer systems.
- ***Customer Authentication with 2FA, without sacrificing UX***—Behavioral biometrics are the innovative and reliable way to secure customer accounts. Many national and international banks have started considering keystroke dynamics or touch patterns as a person's unique characteristics for their authorizations.
- ***Criminal profiling***—Behavioral biometric is used by police and FBI investigators to determine the personality and identity of the individuals who may have committed a crime based on their behavior exhibited during the criminal act and matching it with the stored profiles of the criminals.
- ***Jury profiling***—A BB technique used by lawyers and prosecutors, which can predict the action of the particular potential juror based on their current behavior, overall physical and psychological appearance.

- **Plan recognition**—To understand the goals of an intelligent agent by analyzing their observable actions by creating a map of their temporal sequencing.
- **eHealth and Well-being**—In the health care system, it is possible to make the diagnosis based on how a person behaves. For example, monitoring the way the patient is speaking, typing, talking, or engaging in other daily activities. By comparing it with previous data, it is possible to draw appropriate conclusions about the state of the health of a patient.
- **Healthcare services**—For patient management and electronic health records, voice biometrics is used to provide an additional layer of security that prevents unauthorized access to patient records.
- **Avoiding User Carelessness**—It is not very uncommon for a human to make mistakes. Sometimes, mistakes may open the door for malicious intrusions. If this happens, behavioral biometrics will help in quick detection and flagging the intrusion.
- **License Mismanagement**—Although licenses are personal and individual, still users may use them illegally by sharing or stealing. Behavioral biometrics can be used to eliminate the associated risks by ensuring and verifying that only the named persons are using licensed services or products.
- **Contact Center authorization**—The most common use of voice biometrics is in the contact center space where it is useful for verifying and authenticating the callers, which in turn saves time and effort for both the customer and the agent.
- **Preventing account sharing practices**—Many companies are using BB for authentication and fraud prevention purposes. Banking is one of the sectors where behavioral biometrics is now commonly used. It is used to authenticate whether the person using the service is genuine or not.
- **Workforce authentication**—Possibility is to even identify the workers based on the unique behaviors they have while interacting with the devices. This is possible through a true friction-less and less invasive system that can be built using existing hardware capabilities.
- **Customer Onboarding**—The behavioral biometrics provide insights that provide the global organizations an actionable intelligence, that can be used to create a secure and frictionless digital customer authorizations.
- **Online Lending**—Behavioral biometrics combined with machine learning and risk assessment techniques provide a much more innovative approach to online user authentication, which helps the lending organizations to take quick actions and early approvals.
- **Preventing Online and mobile banking Frauds**—Most of the banks and retailers are tracking their users' way of typing, swiping, and tapping on the devices to make behavioral biometric profiles for authorizations. This helps in reducing fraud. For example: The Royal Bank of Scotland has done a collection of

biometric behavioral data, 2 years ago on private banking accounts for wealthy customers. They are now expanding the system to all of its 18.7 million business and retail accounts, to enhance security and stop all the online frauds.

- **Cyber Threat Detection**—Monitoring user behavior is one of the best ways to detect cyber attacks and fraud in real-time. It focuses on detecting anomalous user behavior by continuously monitoring and matching it with the profiles recorded in the system.
- **Access Control Systems**—Behavioral biometric’s GAIT analysis can be used for access control systems very effectively. This monitors the walking patterns of a human and access can only be granted to the building quickly on approved authorizations, especially in congested areas.
- **Endpoint protection**—Behavioral biometrics provides endpoint protection ensuring the whole enterprise to be protected. It enables safe, remote access to the servers, from any end device, used by the workers. Protects both the devices (nodes) as well as the servers.
- **A critical security component for the IoT.**—Passive continuous re-authentication of the users without notifying them is required in IoT for enhanced security. It may even lock the system automatically in case the user is inactive or irregular or anomalous behaviors are observed by the system.

5.1 Behavioral biometric usage timeline

Behavioral biometrics is totally based on artificial intelligence and machine learning. In the 1960s, Dr. Gunnar Fant and Kenneth Stevens created the first model of speech production using X-rays and then in 1970, Dr. Joseph Perkell used those findings to create a speech recognition biometric model.

A timeline of behavioral biometric solutions is given in **Table 3**.

Year	Biometric Used	Used for
BC–220 AD	Use of handprints as evidence in Qin Dynasty	Crime Investigations
The century	Chinese practice of using fingerprints	Personal Identification
1641–1712	Friction ridge skin observations	Plant Anatomy
1856	Observations on permanence	Identification
1886	Observation on fingerprints for Crime scene investigations and criminal identification	Authorization
40’s	Morse code authentication in WWII	Authentication
1942	Telegraph operators unique tapping rhythm	Identification
1949	Iris Patterns	Identification
1959	Computer’s ability to learn on its own, without human intervention	Learning

Year	Biometric Used	Used for
1960	First model speech production using X-rays of speaking subjects	Authentication
1960	Facial recognition	Identification
1965	Signature recognition system	Identification
1970	Dynamic signature and fingerprints recognition	Identification
1970	An early form of biometric modeling using full-motion x-rays and the previous work of Drs. Fant and Stevens, even used today	Authentication
1980	Speech Group to promote voice recognition tech	Recognition
1991	Real time face recognition	Recognition
1996	Hand geometry recognition gets deployed at Olympics	Identification
1999	ICAO initiates study on biometrics and MRTD	Issuance and acceptance
2001	Face recognition is deployed at the Super Bowl	Recognition
2001	attacks on the World Trade Center draw attention to the need for continuous authentication as a new security measure in global information systems	Security
2002	DARPA launches Total Information Awareness (TIA), the first large-scale use of technologies designed to mine data sets for identifying biometric information	Identification
2004	US-VISIT (United States Visitor and Immigrant Status Indication Technology) becomes operational	Authorization
2006	innovative new algorithms to rapidly and transparently identify computer users as they work	Continuous authorization
2010	Keystroke Dynamics embedded in consumer products	Authorization
2011	Osama bin Laden's body gets identified with biometrics	Identification
2013	Mobile biometrics	Authorization
Mid 2010s	Continuous authentication for mobile application security	Authorization
Mid 2010s	Biometric systems to improve security as well as the system performance	Authorization
Late 2010s	Electric vehicles with face biometrics	Authorization
2018	World's first phone with under-display fingerprint sensor	Identification

Table 3.
Behavioral biometrics timeline.

6. Conclusion

Behavioral biometrics technologies are promising solutions that are designed to complement and improve systems security that is mainly based on physical biometrics. Behavioral biometrics is based on the analysis of unique parameters such as body movements, keystroke dynamics, and device-based gestures. The very common predictions about behavioral biometrics are its increased adoption for authorization, enhance proactive cyber security, and more accurate anomaly detection.

Behavioral biometrics can bring significant benefits to organizations and users. Moreover, it can also be used in emerging fields, such as improving the security of the internet of things, in addition to several traditional environments.

Although there are several challenges in the development and adoption of behavioral biometric systems, they are becoming more popular solutions as they work seamlessly without user intervention and special hardware requirements. Additionally, since the behavioral biometric system cannot be easily fooled using stolen data as the authentication happens dynamically, it provides increased security and convenience. The biggest challenge that faces the adoption of such systems is the need to constantly retrain their classification models to maintain high accuracy rates. Users' behavioral patterns can change based on many parameters, such as emotions, again, illness, etc. Moreover, if the behavioral biometrics depends on sensors or smart devices to collect raw data, such as in keystroke dynamics, then the classification models need to create a new profile every time a user uses a new device. This constant re-training requires the utilization of advanced machine learning techniques, such as re-enforcement learning. Despite these challenges, behavioral biometrics are becoming more popular every day and the market trends show that they are here to stay.


IntechOpen

Author details

Mridula Sharma* and Haytham Elmiligi
Computing Sciences, Thompson Rivers University, Kamloops, BC, Canada

*Address all correspondence to: msharma@tru.ca

IntechOpen

© 2022 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

- [1] Singh JP, Jain S, Arora S, Singh UP. A survey of behavioral biometric gait recognition: Current success and future perspectives. *Archives of Computational Methods in Engineering*. 2021;**28**(1): 107-148
- [2] Sultana M, Paul PP, Gavrilova M. A concept of social behavioral biometrics: Motivation, current developments, and future trends. In: 2014 International Conference on Cyberworlds. Cantabria, Spain: IEEE; 2014. pp. 271-278
- [3] White paper: Behavioral biometrics. Technical Report MSU-CSE-06-2, International Biometrics Identity Association, 1090 Vermont Avenue, NW • 6th Floor Washington, DC 20005, January 2006
- [4] Habeeb A. Comparison between physiological and behavioral characteristics of biometric system. *Journal of Southwest Jiaotong University*. 2019;**54**(6):1-9
- [5] Yampolskiy RV, Govindaraju V. Taxonomy of behavioural biometrics. In: *Behavioral Biometrics for Human Identification: Intelligent Applications*. Hershey: IGI Global; 2010. pp. 1-43
- [6] Alsaadi IM. Study on most popular behavioral biometrics, advantages, disadvantages and recent applications: A review. *International Journal of Scientific & Technology Research*. 2021; **10**(01):15-21
- [7] Liu S, Silverman M. A practical guide to biometric security technology. *IT Professional*. 2001;**3**(1):27-32
- [8] Choi M, Lee S, Jo M, Shin JS. Keystroke dynamics-based authentication using unique keypad. *Sensors*. 2021;**21**(6):2242
- [9] El Zein D, Kalakech A. Feature selection for android keystroke dynamics. In: 2018 International Arab Conference on Information Technology (ACIT). Werdanye, Lebanon: IEEE; 2018. pp. 1-6
- [10] Halakou F. Feature selection in keystroke dynamics authentication systems. In: *International Conference on Computer, Information Technology and Digital Media*. Tehran, Iran: Research Gate; 2013
- [11] Qi Y, Jia W, Gao S. Emotion recognition based on piezoelectric keystroke dynamics and machine learning. In: 2021 IEEE International Conference on Flexible and Printable Sensors and Systems (FLEPS). Manchester, United Kingdom: IEEE; 2021. pp. 1-4
- [12] Ghosh S, Hiware K, Ganguly N, Mitra B, De P. Emotion detection from touch interactions during text entry on smartphones. *International Journal of Human-Computer Studies*. 2019;**130**: 47-57
- [13] Ahmed A, Traore I. Mouse dynamics biometric technology. In: *Behavioral Biometrics for Human Identification: Intelligent Applications*. Hershey: IGI Global; 2009. pp. 207-223
- [14] Antal M, Fejer N, Buza K. SapiMouse: Mouse dynamics-based user authentication using deep feature learning. In: 2021 IEEE 15th International Symposium on Applied Computational Intelligence and Informatics (SACI). Timisoara, Romania: IEEE; 2021
- [15] Monaro M, Cannonito E, Gamberini L, Sartori G. Spotting faked 5 stars ratings in e-commerce using mouse

dynamics. *Computers in Human Behavior*. 2020;**109**:106348

[16] Bhatnagar M, Jain RK, Khairnar NS. A survey on behavioral biometric techniques: Mouse vs keyboard dynamics. *International Journal of Computer Applications*. 2013;**975**:8887

[17] Chellappa R, Veeraraghavan A, Ramanathan N. *Gait Biometrics, Overview*. US, Boston, MA: Springer; 2009. pp. 628-633

[18] Elgammal A. *Gait Recognition, Motion Analysis for*. US, Boston, MA: Springer; 2009. pp. 639-646

[19] Estrela PMAB, Albuquerque RO, Amaral DM, Giozza WF, Nze GDA, de Mendonca FLL. Biotouch: A framework based on behavioral biometrics and location for continuous authentication on mobile banking applications. In: 2020 15th Iberian Conference on Information Systems and Technologies (CISTI). Seville, Spain: IEEE; 2020. pp. 1-6

[20] Yampolskiy R, Govindaraju V. Game playing tactic as a behavioral biometric for human identification. In: *Behavioral Biometrics for Human Identification: Intelligent Applications*. Hershey: IGI Global; 2010. p. 385

[21] Zhanna Korotkaya. Biometric person authentication odor. *Semantic Scholar*; 2003:1

[22] Borowik P, Adamowicz L, Tarakowski R, Siwek K, Grzywacz T. Odor detection using an e-nose with a reduced sensor array. *Sensors*. 2020; **20**(12):3542

[23] Amin MA, Yan H. Gabor wavelets in behavioral biometrics. In: *Behavioral Biometrics for Human Identification: Intelligent Applications*. Hershey: IGI Global; 2010. pp. 121-150

[24] Plamondon R, Srihari SN. Online and off-line handwriting recognition: A comprehensive survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2000;**22**(1): 63-84

[25] Ravanelli M, Bengio Y. Speaker recognition from raw waveform with sincnet. In: *IEEE Spoken Language Technology Workshop*. Ithaca, New York: IEEE; 2019

[26] Moskovitch R, Feher C, Messerman A, Kirschnick N, Mustafic T, Camtepe A, et al. Identity theft, computers and behavioral biometrics. In: 2009 IEEE International Conference on Intelligence and Security Informatics. Richardson, TX, USA: IEEE; 2009. pp. 155-160

[27] BioCatch. 2021. <https://www.biocatch.com> [Accessed: December 2021]

[28] Simprints [Online]. 2011. Available from: <https://www.simprints.com/> [Accessed: November 29, 2021]

[29] Plurilock [Online]. 2016. Available from: <https://www.plurilock.com/>

[30] VERIFY 2FA [Online]. 2014. Available from: <https://www.typingdna.com/verify> [Accessed: December 14, 2021]

[31] TypingDNA [Online]. 2016. Available from: <https://www.typingdna.com/> [Accessed: November 10, 2021]

[32] ActiveLock [Online]. 2016. Available from: <https://www.typingdna.com/activelockcontinuous-authentication> [Accessed: November 30, 2021]

[33] Focus [Online]. 2016. Available from: <https://www.typingdna.com/focus> [Accessed: November 2, 2021]

- [34] ThreatMark [Online]. 2015. Available from: <https://www.threatmark.com/whythreatmark/> [Accessed: December 2, 2021]
- [35] 3Divi [Online]. 2011. Available from: <https://www.3divi.com/> [Accessed: November 29, 2021]
- [36] Zighra. Zighra Smart Identity Defense [Online]. Ottawa, ON, Canada: Zighra; 2010. Available from: <https://zighra.com/> Accessed: December 2, 2021
- [37] Deepak Dutt. Government of Canada Awards Innovation Contract to Zighra to Pilot Continuous Authentication for Remote Access using Patented Next Generation AI Technology, OTTAWA, ON; 2021. Available from: PRNewswire.com
- [38] Aculab. VoiSentry: Easily add Speaker Verification and Authentication to your Applications. UK & USA: Aculab; 2018 Available from: <https://www.aculab.com/>
- [39] Cynet. Monitor User Behavior to Discover Compromised Identities [Online]. 2018. Available from: <https://www.cynet.com/platform/threatprotection/uba-user-behavioranalytics/> [Accessed: November 29, 2021]
- [40] Burkhard Stiller, Thomas Bocek, Fabio Hecht, Guilherme Machado, Peter Racz, and Martin Waldburger. Protect Users Without Frustrating Them Using AI-Driven Behavioral Biometrics. Technical report, 01 2010
- [41] SecureAuth. Identity Security Without Compromise [Online]. 2014. Available from: <https://www.secureauth.com/> [Accessed: December 14, 2021]
- [42] UnifyID - authentication, reinvented [Online]. 2015. Available from: <https://unify.id/index.html> [Accessed: December 14, 2021]
- [43] Securetouch [Online]. 2016. Available from: <https://craft.co/securedtouch> [Accessed: November 29, 2021]
- [44] Grand View Research. Press Release: Behavioral Biometrics Market Size Worth \$4.62 Billion by 2027. San Francisco, United States: Grand View Research; 2020 Available from: <https://www.grandviewresearch.com/>
- [45] Amigud A, Arnedo-Moreno J, Daradoumis T, Guerrero A-E. A behavioral biometrics based and machine learning aided framework for academic integrity in e-assessment. In: 2016 International Conference on Intelligent Networking and Collaborative Systems (INCOS). Ostrava, Czech Republic: IEEE; 2016. pp. 255-262