Biometric applications in education

Marcela Hernandez-de-Menendez · Ruben Morales-Menendez · Carlos A. Escobar · Jorge Arinez

Received: 26 November 2020 / Accepted: 22 July 2021 / Published online: 28 July 2021
© The Author(s), under exclusive licence to Springer-Verlag France SAS, part of Springer Nature 2021

Abstract
Educational institutions are acquiring novel technologies to help make their processes more efficient and services more attractive for both students and faculty. Biometric technology is one such example that has been implemented in educational institutions with excellent results. In addition to identifying students, access control, and personal data management, it has critical applications to improve the academic domain’s teaching/learning processes. Identity management system, class attendance, e-evaluation, security, student motivations, and learning analytics are areas in which biometric technology is most heavily employed. A literature review is performed to present an overview of biometric technology applications for educational purposes, challenges that must overcome to implement biometric technology, and potentially foreshadowing trends effectively. The future seems promising for biometric technology; the biometric technology market is expected to reach a value of USD 94 billion by 2025 at a compound annual growth rate of 36%. New characteristics are under development for commercial applications, such as vascular pattern recognition, ear shape recognition, facial thermography, odor sensing, gait recognition, heartbeat authentication, brain waves, and human body bioacoustics. The biggest challenge this technology must overcome is security and privacy issues, which must be addressed to fully develop the technology to its full potential. It is desirable that this literature review can provide researchers with a sound vision of the potential that biometric technology will have in education.

Keywords Educational innovation · Higher education · Biometrics · State of the art

1 Introduction

Educational institutions are transforming themselves to be more flexible and adaptable to respond to actual social demands. They are acquiring novel technologies to help them make processes more efficient and services more attractive for students and faculty (and society). Competency-based teaching is oriented to progressive and gradual learning of knowledge, skills, attitudes, and values, which requires real experiences in the educational process.

Generational changes have rendered it necessary for universities to understand and adapt to student’s requirements and expectations. Generation Z (GenZ), born in 1995, grew up during the technological revolution (internet, social networks, etc.). Thus, they are easily linked to the virtual world [14]. GenZ has some common characteristics: creativity, self-taught, multi-screen, and multi-tasking. Therefore, they represent a challenge for traditional education:

- 47% of GenZ spends more than 3 h a day on a video platform.
- 59% uses YouTube to learn.
- 39% prefer to attend a class with a teacher [52].

Their pragmatism distinguishes GenZ, adaptability to work conditions, and integration with other generations (Baby Boomers, GenX, and Millennials). This generation brings new challenges for education, new uses of technology (and new technology), new ways of teaching and evaluating,
and new digital platforms. These new educational tools and approaches have only been accelerated in response to the Covid-19 pandemic.

Educational institutions have implemented various technological tools, including virtual and augment reality, the internet of things, artificial intelligence, 3D printing, telepresence, blockchain, and biometrics [28]. However, the last one is gaining the attention of the educational community as biometric identification systems are becoming popular.

Biometric “is the science of analyzing physical or behavioral characteristics specific to each individual to authenticate their identity.” In a few words, it measures the human body. This technology can measure physiological (e.g., fingerprints, vein patterns, iris, retina, the shape of the hand and shape of the hand) and behavioral traits (e.g., voice recognition, gait, gestures, the sound of steps, and signature). A combination of characteristics can also be made as a multi-modal biometric, which improves measurement confidence. Such combinations could be face and fingerprint, face and iris, etc. The main benefit of biometric technology is that it collects unique human characteristics for each person [64].

Biometric systems have characteristics that allow for their use in different domains. Several government initiatives (e-passports, e-driver’s licenses, border management, and national identifications) are being implemented using advanced biometrics. The banking sector has improved security by using biometric technologies (fingerprint scanners, facial/voice recognition, etc.) to track its customers. Banks also use biometrics to authenticate and protect customer’s financial data; it is a long-term market change. With the Internet of Things (IoT), collecting and storing patient data in hospitals has become easier/safer; however, biometric technology can significantly improve. Biometrics can improve essential aspects such as patient’s identity and support with real-time information to offer adequate medical services. Facial recognition, iris, and finger scanners are examples of biometric technologies used to access or control a patient’s data.

Regarding the security and privacy of patient data, biometrics helps in monitoring and documentation. The productivity of medical personnel (nurses, doctors, etc.) can also be monitored using biometrics. The hotel industry is adopting this technology to achieve a strategic differential in this highly competitive sector. This technology (fingerprint scans or facial/voice recognition) allows hotels to efficiently automate guest’s identification and access and make their stay more comfortable and safe. Using biometric technology, the entry in the migration processes in airports can be accelerated while maintaining security. Many systems use fingerprint scanners, a very efficient and safe tool. Many retailers rely on biometric technology (facial recognition) to prevent theft or promote customer-related items based on their views and interests in a product (Sharman, n.d.). There are platforms such as elBio that are built to teach students about biometric technology. This system introduces the field through a tutorial, and real interactions with verification and identification processes are performed [59]. Hand geometry systems are helpful to allow access to university systems [51].

Biometrics is not a new technology. This science dates back to ancient Egypt, where pharaohs relied on height measurements to verify their identity. They also authenticated the decrees they issued by adding their fingerprint to a document and their signature [4]. Figure 1 indicates the criteria that must be met for a physiological or behavioral attribute to be used as a biometric trait [33].

A classification of the characteristics measured with biometric systems is presented in Table 1 [68]. In addition, feature sets are included between braces [{}].

Biometric technology is also used for recognizing individual human identities, including DNA, retinal, iris,
Table 1 Classification of biometric characteristics [feature set]

| Hand region              | Facial region                        | Ocular region                          | Medical-chemical | Behavioral                      | Soft  |
|--------------------------|--------------------------------------|----------------------------------------|------------------|---------------------------------|-------|
| **Finger Print**         | Face                                 | Retina                                 | Body             | Keystroke Dynamics              | Gender|
| [Ridge flow, ridge pattern, singular points, ridge skeleton, ridge flow, ridge ending, ridge contours, ridge kernel, orientation field, island, spur, crossover, learned feature, sweat pores, dots and incipient ridges] | [Distance between eyes, mouth, side of the nose, face image, corner points, contours, gender, goatee, roundness face, edge maps, pixel intensity, local and global curvatures] | [Vein bifurcations, area of optic disk or fovea] | [Keystroke duration, hold time, keystroke latency, speed, pressure, digraph latency] |       |
| **Palm Print**           | Ear Shape                            | Sclera Vasculature                      | Odor             | DNA                             | Ethnicity |
| [Ridges, singular points, minutiae points, principal lines, wrinkles, palm texture, mean, variance, moments, center of gravity and density, spatial dispersivity, L1-norm energy] | Size, length, width & height of helix rim, triangular fossa, anti-helix, concha, lobule, step edge magnitude, color, curvature, contours, edge information, shape indices, registered color, range image pair] | [Vein bifurcations] | [Color, shape, and iris texture (crypts, furrows, corona, freckles)] |       |
| **Hand Vein Pattern**    |                                      |                                        |                  |                                 | Height  |
| [Vein bifurcation and ending] |                                      |                                        |                  |                                 |        |
| **Finger Knuckle**       |                                      |                                        |                  |                                 |        |
| [Texture of lines, orientation, magnitude] |                                      |                                        |                  |                                 |        |
| **Hand Geometry**        | Tongue Print                         |                                        |                  |                                 |        |
| [Length and width fingers, aspect ratio finger or palm, length, thickness & area hand, hand contour, hand coordinates and angles, Zernik e moments, skin-folds and crease pattern] | Width, thickness, the curvature of tongue contour, cracks, texture] |                                      |                  |                                 |        |
| **Tongue Print**         |                                      |                                        |                  |                                 |        |
| **Teeth**                |                                      |                                        |                  |                                 |        |

The bold words are use to highlight the biometric characteristics
voice, facial images, fingerprints, and handprints. It scans one of the above characteristics and compares them with stored data. The most common features used are fingerprints and iris. Fingerprints are likely a standard method because fingerprint scanners are relatively inexpensive [40]. Fingerprint scanners are applied in everyday activities, such as access control and vehicle driver license registration. Research in iris biometrics has accelerated since 2001, with its peak occurring in 2006.

Features such as the face, voice, and retina are also employed. Face biometrics is fast, inexpensive, and non-intrusive. It is also a robust technology that is not heavily influenced by the environment. Researchers have also been working on voice systems to understand the personal encoding of natural languages. In addition, voice biometrics can work with standard telephones, making it a versatile option [77].

Behavioral biometrics provide several advantages over traditional biometric technologies (iris, fingerprint, handprints, etc.). They can be collected non-obtrusively or even without the knowledge of the user. The collection of behavioral data often does not require any specialized hardware and is very cost-effective. While most behavioral biometrics are not unique enough to provide reliable human identification, they have been shown to give sufficiently high accuracy identity verification. Unfortunately, this type of biometric is not as popular as traditional biometric systems. The reason could be that behavioral characteristics are not exact enough to identify people. However, they have many advantages, such as analyzing people in their routine activities and collecting information that includes a time dimension. The behavior is quantified, and results are used to verify the identity of the person. Some behavioral biometric examples include facial features, email behavior, game strategy, lip movement, mouse dynamics, painting style, programming style, signature/handwriting, storage activity, and systems calls [75]. Biometrics can also be used for verification or identification processes. In the former, a person that claims identity is verified or rejected. An unknown sample is matched with the stored data [5].

A basic biometric system is a pattern recognition system that matches the acquired image’s salient or discriminatory features with stored image’s features. It comprises five main modules, contained in Fig. 2 [19, 68].

A biometric system works in verification or identification mode. In the verification mode (or positive recognition), a user submits the biometric trait and particular identity to the confirmation system. The recognition system validates or voids the user’s claim by comparing (one-to-one) the proposed biometric feature and stored biometric feature associated with the identity. In identification mode (or negative recognition), the system tries to recognize the user by comparing the submitted biometric feature to all the stored biometric features in the database by making (one-to-many) comparisons without a specific identity claim.

The recognition systems based on the measurement of a single biometric modality cannot guarantee 100% accuracy, as shown in Table 2 [68]. This is due to several factors: (1) noisy data, (2) class variation, (3) distinctiveness, (4) non-universality, and (5) false identity. One solution to this challenge is to use multiple and independent biometric modalities that offer more robustness in precision. A multimodal biometric system may involve multi-sensors, multi-algorithms, multi-instances, multi-sample, multimodal systems. This approach could be serial or cascade mode and with different fusion levels: sensor, feature, matching score, or decision.

Multimodal processes are done through different devices/sensors that can be used to collect biometric data; these include: (a) cameras for facial or iris recognition, (b) scanning devices for fingerprint recognition, (c) smartphones and laptops for fingerprint recognition, (d) telephones and microphones for voice recognition, (e) special tablets and a digital pen for signature recognition, and (f) keyboard device for keystroke dynamics [15, 16].

The biometric market is expected to reach a value of USD 94 billion by 2025, at a compound annual growth rate of...
36%, during the next 5 years. This is due to a paradigm shift in commercial discourse, seeking new comprehensive solutions, more privacy, and fewer security threats. Vendors of biometric solutions include: JayPeetek Inc., SecuGen® Biometric Solutions, onClick® Corp, etc. which offer biometric mice [40], Gladstone Education offers identity management systems; Squidcard provides a cashless payment system using fingerprint; Voice Commerce offers voice authentication services [23], and Newcastle-based ievo Ltd is a producer of advanced biometric fingerprint readers who is very demanded by schools and also nurseries [18]. The benefits of using biometric systems vary, including increased security, increased convenience, reduction of fraud, and delivery of enhanced services [77].

A literature review is performed to present an overview of biometric technology applications for educational purposes. The paper outline is as follows: Sect. 2 describes the applications biometrics offers in the academic field. Section 3 presents the challenges that must be overcome to implement the technology under consideration effectively. Section 4 presents the trends that are foreseeing. Finally, Sect. 5 concludes the paper.

2 Applications in education

Biometrics technology is gaining momentum. In 2001 the MIT Technology Review considered biometrics a world-changing emerging technology [59]. Biometric technologies are disrupting several industries and sectors. General applications include its use for recreational activities, such as in Disneyland. It can also be used for replacing password systems. Innovative devices have also been developed, such as a mouse that recognizes the fingerprint of its owner. ATMs also use this technology [40].

There is also another exciting field of biometrics, in which the emotional and cognitive state of people are detected. This can be used to monitor student’s behavior/emotions and change the educational process appropriately. For example, researchers argue that boredom negatively influences learning, whereas engagement improves learning outcomes; biometric sensors have been used to measure electrodermal activity, skin temperature, and heart rate, all good predictors of emotions [73]. Biometrics allows academic institutions to save time, money and also improve educational and non-educational activities. They also offer convenience, safety, and security. Various applications are identified: school access, control of attendance, food service, access to library and media center, bus transportation, control staff time, among others (Fry and Dunphy, n.d.). In addition to identifying students, access control, and personal data management, it has critical applications to improve teaching/learning processes in the educational domain, Fig. 3.

### Table 2 Standard accuracy for different biometric modalities

| Biometric modalities | Accuracy (%) | Applications |
|----------------------|--------------|--------------|
| Fingerprint          | 99.9         | Border Control (BC), Forensics (F), Criminal Identification (CI), Access Control (AC), Computer Logins (CL), E-Commerce (EC), Welfare Disbursements (WD), Missing Children Identification (MCI), IdCards (IC), Passports (P), User Authentication (UA) on mobile devices, Time and Attendance Monitoring Systems (TAMS) |
| Iris                 |              | BC, CI, AC, CL, EC, WD, MCI, IC, P, TAMS |
| Vein pattern         | 99           | AC, EC, UA |
| Retina               |              | BC, CL access control in susceptible installations |
| Palmprint            | > 95         | AC, EC, CL, UA, TAMS |
| Hand geometry        |              | BC, F, CI, AC, CL, EC, WD, MCI, ID, P, video surveillance, crowd monitoring |
| Face                 |              | AC, EC, CL, TAMS |
| Ear                  | > 90         | AC, EC, CL, UA |
| Voice                |              | CL, UA |
| Keystroke dynamics   |              | Video surveillance, F, CI from video sequences, UA |
| Signature            |              | AC, CE, CL, e-banking |
security reasons, as it can grant access to a given system to only authorized persons, identified by their physical or behavioral characteristics [59]. Fingerprint cards are already used in schools for students that acquire free meals in coffee shops [23]. Indeed, the use of fingerprints is a common practice from elementary school to universities/research centers.

Nita and Mihailescu [48] proposed a secure e-learning system based on biometric authentication and homomorphic encryption exploiting cloud computing. Additionally, this proposal predicts if he/she would pass a final exam based on past data of the user’s behavior (using biometrics data).

2.2 Class attendance

With biometrics, the attendance of students to a given class can be accelerated. This is advantageous since time devoted to taking attendance is reduced. Also, a more accurate registration process can be performed, diminishing errors [9]. This technology also enables identifying causes and patterns of absence, and the behavioral characteristics of students can be correlated with class achievement. Analysis of absence between year groups and groups of individuals can also be performed. Universities can also use this technology to track students [60].

The University of Sunderland London Campus is already using this technology to report class attendance. They use a portable device that has a fingerprint sensor. When students enter the class, they put their fingers on the device to easily register their presence. In India, Delhi University uses this system to track professors’ attendance to class [10]. In addition, researchers used a biometric fingerprint device to improve active class participation in those classes that consist of a pure lecture. It was combined with a rewarding activity resulting in improved student engagement and class results [32]. Finally, this technology can also be used in online activities or education to manage time effectively [29].

2.3 e-Evaluation

The submission of e-exams is a relatively new use of biometrics (i.e., since 2017). However, research in this area has been headed by international organizations such as the European Union with its project Adaptive trust-based E-system Assessment for Learning. In these projects, 17 European organizations use keystroke and facial recognition technologies to identify university student’s identities and reduce cheating [25].

Fingerprint recognition can be used for students to take online exams. In this case, learners must verify their identity, and only after that, the exam can be shown on the screen. This can be done by identifying them through facial, iris, or voice recognition. Either the characteristic used, a student sample must be first taken to perform the matching process [15, 16].

Biometric systems (finger scans) to verify the identity of IELTS test takers have been implemented globally. As a result, IELTS is available in over 900 locations in 130 countries, making the British Council and IDP IELTS [10].

2.4 Security

Biometrics is a useful technology to identify students and ensure no outsiders either in class or on the university’s campus. On the other hand, this technology can be used in combination with surveillance cameras to detect strangers. In addition, a blocking protocol can be activated in an emergency on campus to ensure that no one enters or
leaves. Using identification chips (based on radio frequency) and combining them with intelligent data, students can be located to guarantee their safety. Biometric systems can also limit access to computers, emails, websites, and other restricted educational tools (assessments) [29]. Finally, students’ presence on campus can be tracked by knowing at any time where they are, when they arrived and left, and where they went [18].

Higher Education is becoming one of the most popular targets for cyberattacks because universities have relatively open networks. For example, universities have several wireless networks that connect their areas using multiple bandwidths; these multiple networks lead to an output that contains student data (payment information, social security number, personal addresses, etc.). Additionally, universities must comply with various laws to protect student data; these laws’ guidelines may restrict the institution’s IT infrastructure or leave it vulnerable to hackers (Bio-KeyTM, n.d.).

The computer industry is changing rapidly, and people are pushing toward a new technological system buying the latest editions of phones and computers. However, inexperienced users coming into technology rapidly, many of them could unintentionally expose information without realizing it. An inexperienced user can potentially be subject to scams, spoofing, and phishing because the university network allows hackers to enter and exit a system without being detected swiftly. Educational institutions establish an open network architecture with multiple access points; if someone misplaced their cellular phone, a hacker could potentially log into the system and access the entire mainframe.

If intellectual property (patents, documented permission) is stolen, it could cost the institution a large amount of money. Faculty and student personal identification are available; it includes healthcare, credit card/payment, etc. Also, students and faculty have highly sensitive data (bank accounts, personal addresses, etc.). There are many government regulations that Higher Education institutions must follow. Still, in doing so, they expose themselves to a possible attack that they cannot stop due to the regulations. Cyber attacks in Higher Education date back to 2002, Table 3 [41]. The hackers’ goal remains personal data, social security numbers, financial information, opening up a new credit card, collecting tax refund, etc.

Biometrics enable body-based security—a technology that authenticates identity based on physical characteristics such as fingerprints, irises, facial structure, voice, and even gestures. Fingerprint authentication (the most commonly used biometric technology) is based on a unique set of identification. Instead of using a passcode, only one person can log into a system using this biometrics technology. Students can start using their fingerprints as their credentials for several reasons: (a) the authentication rarely fails, (b) fingerprints do not rely on memory, (c) rapid system recognition of the fingerprint. By establishing fingerprint authentication, biometrics can protect network architecture and access to other areas. Biometrics is going to be the most powerful technology against cyber-attacks in Higher Education.

| Year | University                          | Description                                                                                     |
|------|------------------------------------|-------------------------------------------------------------------------------------------------|
| 2002 | Yale University                    | The first cyberattack in higher education was by hackers from Princeton University; the goal of espionage was information about admission decisions |
| 2004 | California Universities            | About 2,000,000 records were stolen through 3 infractions. Personal data was the main target    |
| 2005 | University of Hawai                   | A previous librarian stole the personal data of 150,000 students, staff, and library patrons to obtain loans |
|      | University of Utah                  | About 100,000 names and social security numbers of former employees were stolen from databases |
| 2006 | UCLA                               | The cyberattack resulted in the loss of around 800,000 records of faculty, staff, parents, and student applicants |
| 2007 | Florida A&M University              | Three hackers used keylogging software into the PeopleSoft system to steal passwords; the goal was changing the grades |
| 2008 |                                 | The size of cyberattacks into the PeopleSoft system increased significantly—10 times             |
| 2012 | University of Nebraska              | A student accessed the database, critical information of 654,000 students and employees was accessed |
| 2013 | Massachusetts Salem State Univ      | The goal was personal data                                                                      |
| 2014–2016 |                                 | The frequency of security violations affecting universities multiplied by almost ten [71]       |
| 2017  |                                   | The number of cyber-attacks increased to almost 400                                              |
| 2018  | More than 300 universities worldwide | Nine Iranian hackers accessed 31 TB of valuable intellectual property and data                   |
2.5 Understand students’ motivation and academic progress

In addition to knowing the course’s educational content, a good teacher must know their students very well and identify their cognitive status to guide the teaching–learning process properly. For example, if the teacher determines the student’s commitment or motivation, he can use different educational strategies to optimize the teaching process. However, when the educational process is done remotely, and for many students, automated system’s support is required. This is where biometric technology opens up an excellent opportunity to develop strategies that help detect student’s cognitive states.

Due to their influence on learning, emotional states play a crucial role in education in general. Boredom has been shown to influence learning, while engagement can positively improve learning outcomes. Frustration and confusion can positively affect learning if the student can resolve these states. Estimating prediction in real-time of student’s affective states is a research topic of great interest due to its benefits through different intervention strategies [24]. The collection of appropriate biometric data and the analysis of physiological and behavioral patterns during a learning experience can help introduce proper interventions to improve the learning experience as the main hypotheses in this domain.

Biometrics provides an objective measure of the physiological reactivity of users that is used to infer affective states. Electrodermal activity, skin temperature, and heart rate showed high performance as predictors of emotions [34, 35, 55]. Wampfler et al. [73] predict a student’s affective states (while solving math exercises) using arbitrary writing and drawing assignments (based on stylus data).

A low-cost mobile setup to detect student’s affective states (non-intrusive and minimum issues related to privacy) is proposed. The system considers bio-sensor data from skin conductance, heart measures, and skin temperature with handwriting data recorded by a stylus to predict student’s affective state in a valence-arousal space of emotions proposed [54]. Valence describes how much emotion is perceived as positive/negative, and arousal represents the emotion’s intensity. The circumplex model has two dimensions representing affective states in terms of valence/arousal. The circumplex model has the leading eight affective states (Arousal-0o, Excitement-45o, Pleasure-90o, Contentment-135o, Sleepiness-180o, Depression-135o, Misery-270o, and Distress-315o). The pleasantness-unpleasantness and arousal-sleep dimensions account for the significant proportion of variance; the dimensions of the effects are bipolar; any effect could be defined as combining pleasure and arousal components. Recorded stylus and bio-sensor data are preprocessed, and the relevant features are extracted to train a classification model (using the Random Forest algorithm) for the specific affective regions. Early results are very promising and practical; however, more experiments and validations are required to have overall effects in other knowledge and educational settings.

Dafoulas et al. [13] used a range of sensors measuring critical data from individual learners, including heartbeat, emotion detection (anger, disgust, fear, happiness, sadness, and surprise), sweat levels, voice fluctuations, and duration/pattern of contribution via voice recognition. Employing biometrics for supporting assessment, facilitating, and enhancing learning experiences in collaborative learning.

Smart biosensors and cameras (infrared) can identify and track students, diagnose their behavioral state (body language and eye contact) and their peer’s actions. This can aid in making opportune changes in the teaching–learning processes and improve students’ results. Also, online student engagement diagnosis will help teachers use the needed teaching strategies and technologies to optimize student’s learning.

Many scientific projects have been developed to investigate and estimate student’s cognitive states during the teaching/learning processes, based on data and evidence using biometric technology. With this information, the educational process can be optimized. Preliminary results are reasonable; however, research must continue to obtain general, practical, and valid conclusions in different domains. Based on biometric technology, it is possible to assess a student’s academic progress and customize strategies to help him achieve his goals [29].

2.6 Biometrics in learning analytics

Learning Analytics is defined as measuring, collecting, analyzing, and reporting data about students and their learning contexts to understand and optimize the learning process and the learning environment [58]. Learning Analytics is an area of technology-enhanced learning. Big data, cloud technologies, virtual reality, brain-computer interface are some of the technologies that powered Learning Analytics.

LA benefits are: (1) prediction of student performance, (2) personalized student experience, (3) student confinement increases, (4) improves e-learning systems, (5) enhances cost-efficiency. To achieve these Learning Analytics benefits, it is necessary to collect data from various sources. Many data sources vary among many fields, including written or online surveys, interviews, students’ opinions, improvements suggestions, web tools, and more sensitive data: biometric data. The focus is on biometric data due to the recent technologies and devices that enable collecting and analyzing such data [15, 16].

Social Network Analysis, GISMO (student-monitoring tool), CourseVis (learning management system), Contextualised Attention Metadata, LOCO-Analyst, Social Networks
Adapting Pedagogical Practice (SNAPP), Honeycomb, Gephi, sense.us, Signals, and GRAPPLE Visualisation Infrastructure Service (GVIS) are some of the Learning Analytics tools that have been developed over time [20].

Secure access to information and data privacy of learners’ data shall be provided as one of the essential issues that biometric-based systems can quickly solve. Brain-Computer Interface (BCI) is a direct communication channel between the human brain and a computer. BCI is a Human–Computer Interface branch oriented towards research human cognitive, sensorial, or motor functions [38]. EEG-based BCI can help focus student attention and memory retention. It can also measure affective states and adapt the challenge difficulty to the learner’s emotions or even measure the engagement level. This area can improve learning and opens up a large area of research to help people with disabilities.

Over time, tracing Learning Analytics development highlights a gradual shift away from a technological focus towards an educational focus. Factors driving the growth of Learning Analytics:

(a) Big data: Significant amounts of learner activity take place, and records are distributed across a variety of different sites with different standards, owners, and levels of access.
(b) Online learning: Learning online offers many benefits, but it is also associated with problems.

3 Challenges

The growth of biometric systems has exponentially developed in education and other application areas; however, some opportunities and challenges must be considered to ensure good results.

3.1 Users reluctant to use the technology

As biometrics is relatively new, users might be reluctant to use it. It could pose various problems such as wide variance when measuring characteristics, affecting the system’s performance. Cultural and social issues must be taken into consideration when designing a biometric system. If not, any initiative can fail. People could be reluctant and fearful of using these systems due since they collect personal information. Also, people may be afraid of acquiring a disease if using, e.g., a fingerprint apparatus (because of the Covid19 pandemic). Some persons might be fearful of how their photographs taken from recognition systems will be managed. Biometric systems that track employee’s movement seem beneficial for the employer but intrusive for the worker [51].

3.2 People that can develop solutions and use the technology

For this technology to advance, it is necessary to educate future engineers in this technology well. This is important for developing commercial products that are attractive, useful, and at the same time, solve social problems. This could be achieved by incorporating knowledge regarding the technology in the curriculum of Information Technology universities programs. Several universities are already doing their part. For example, West Virginia University offers the first undergraduate program in biometrics; people who acquire a Bachelor of Science degree in Biometric Systems.

On the other hand, the University of Hertfordshire in the UK has already created a Master’s Degree course in Biometric and Cybersecurity. However, as this is a new field of study, it isn’t easy to transmit knowledge effectively. Therefore, some researchers suggest the use of simulation tools.

3.3 Confiability

Biometric recognition is based on statistics; i.e., it does not perform a yes or no decision but provides a match score. This can cause the system to present errors given access to an incorrect person [59]. Environmental issues can also cause errors in the system. Temperature, humidity, and illumination conditions are some of the factors that can influence a biometric system to fail. In physiological recognition, there can be errors during the process, e.g., a student’s voice can be altered due to sickness or a noisy environment during the recognition. Performance errors that can be mentioned include computing good quality images, the composition of the population, and the robustness of recognition algorithms [68].

3.4 Privacy issues

Biometric systems have the potential to collect a vast amount of information about people. Privacy is a concern that students and parents have regarding the use of biometric systems in schools. For example, finger and palm print biometric can track individual’s dietary habits, which can be intrusive. In 2002, schools in the UK began to scan fingerprints of children without asking for parental consent. These are some of the events that make the academic community have fear mainly about the uses that the data collected will have [9]. However, there are biometric systems that do not necessarily store images of the characteristics being used. For example, in fingerprint recognition, a number is given to a student’s fingertip when the first pass in the biometric device. The number is again generated for subsequent reads and compared with the numbers stored, identifying the student if there is a match [60]. In e-learning, where a person...
can learn at every moment, it is crucial to ensure that the personal data collected is safe and provides a personalized experience [15, 16]. Therefore, biometric systems should incorporate privacy-protective solutions in their architecture. These should allow a system to work appropriately and give the users confidence and keep personal information safe [77].

3.5 Improvement of biometric technology

Biometric sensors should provide high-quality data that meet standards in mobile and challenging environments. Also, these should work by collecting data from faraway places, i.e., at a distance. Biometric systems should be increasingly accurate regardless of the environment in which they are doing [77]. Matching algorithms should also be improved, so they work in the presence of imperfect segmentation, noisy features, and signal variance. On the other hand, the technology should be robust enough to face attacks that include falsified biometric traits [51]. These systems are vulnerable due to their components, such as capture devices, communication channels, and databases. It is essential to improve these issues to work efficiently enough [62].

3.6 The new reality after CoViD19

Humanity before the Covid19 lockdown now seems to have passed a lifetime, and the psychological impact of what we are currently experiencing is likely to be enormous, even incalculable proportions. Facial recognition was promoted as one of the significant changes brought about by the coronavirus pandemic. To counter-balance identification problems due to partial face concealment, biometric Machine Learning and Artificial Intelligence algorithms are being pushed to the next evolutionary step [11].

CovidTech is a new technology and data movement due to the coronavirus pandemic. CovidTech constitutes the broadest and most profound period of agile technology and data development involving personal data processing.

There are two critical issues at CovidTech: epidemiology and exit strategies from the lockdown. Facial recognition is a crucial part of CovidTech. For example, buses in China have facial recognition systems that are combined with bus thermometers. Russia redesigned its facial recognition technology. Apps are being developed in Poland and India to allow people to upload selfies to contribute to the facial recognition system. Contact tracing is a proven epidemiological technique that has worked successfully in other health emergencies. These are only some examples of the CovidTech solutions that have potential in Higher Education Institutions, but there are certainly some contact-based Biometrics that no have room now. However, there are legal issues of use and scope that have not yet been resolved (Room, 2020).

3.7 Some societal and ethical issues

Technology improves the limits of our abilities but challenges our moral boundaries. Biometrics technology is part of our day; for example, through brain implants, social networks like Facebook, etc., using big data and emotion recognition, some systems learn to behave like humans [69].

Biometric systems allow the use of unique physical characteristics for verification or identification purposes. But, they invade our socio-cultural world, generating some social and ethical issues. Today, most public and political interests focus on privacy (especially personal data protection) and digital security. An analysis of the scientific literature on biometric systems revealed several recurring themes: privacy, security, autonomy, justice, human dignity, control of technology, and balance of powers. The various ethical and social problems manifest themselves in different ways. We will briefly comment on some examples to raise awareness of this issue (Royakkers et al., 2018).

Concerning privacy, biometric technology requires a minimum amount of information to determine if someone has the right to enter a building. On the other hand, because biometrics can identify sensitive data, controlling what happens to that information can be difficult, especially now that the technology has reached the stage of being applied in many more devices and situations. In the example of access to a building, the identity is not revealed; the verification can also be done by comparing someone’s biometric characteristics with the information already stored about that person. Thus, biometrics is an excellent way to demonstrate legitimacy while maintaining privacy.

One application of biometrics is facial recognition and identification used in police investigations; this is regulated by law. This highly sensitive information must be stored securely, as biometric data can contain health (risk) and ethnicity. You don’t want an insurance company to get hold of the information. An iris scan can determine diabetes or high blood pressure. Fingerprint irregularities can indicate leukemia or breast cancer.

The next generation of biometrics not only gives an idea of "who are you" but also answers the question “how do you feel” [45]. Emotion recognition technology provides information about people’s mental state by examining people’s automatic non-verbal comments without knowing it. For example, specific walking, grimacing, and other facial expressions can reveal something about a person and their behavior [17]. Unfortunately, a biometric system can misclassify and stigmatize someone as a terrorist, criminal, or unreliable individual. This can lead to revoking the presumption of innocence, this stigma likely stays with that person [61].
4 Biometric educational trends

Fingerprints, faces, and iris are well-known and consolidated biometric technologies; newer biometrics emerging for different applications include higher education. Although some technologies began to develop many years ago, they have not achieved the proper application level. A brief review is presented with some applications, Fig. 4.

4.1 Vein/vascular pattern recognition

Vascular pattern recognition (vein pattern authentication) uses near-infrared light to reflect images of a person’s blood vessels. The vascular pattern of humans is unique and does not change over the years. The potential for using this technology lies in obtaining trans body images and the possible applications of optical computed tomography scanning [56]. This technology uses subcutaneous blood vessels on the back of the hands or fingers due to their easy access since the near-infrared rays generated by a bank of LEDs can penetrate the skin on the back of the hand. Due to the difference in absorbance of blood vessels and other tissues, reflected near-infrared rays produce a vascular pattern extracted by various image processing techniques. Different feature-rich data (vessel branch points, vessel thickness, and branch angles) are extracted and stored as a template. Some disadvantages of this vein / vascular technology could be that (a) the quality of the captured image can be affected by body temperature, ambient temperature, humidity, uneven heat distribution, heat radiation, the proximity of the vein to the body surface, camera and focus calibration, and (b) this technology is invasive, which can be a significant limitation, especially in times of pandemic.

Compared to other biometric scanners, palm vein recognition technology has reduced false acceptance/rejection rates; improves the speed and security of endpoint contactless authentication [50], mainly due to the continuous development of the sensors used. A biometric finger vein scanner using infrared light and a CMOS image sensor in a specially designed system to reduce optical background noise in vein images are commercial solutions [8]. In addition, NASA developed a new subcutaneous structure imager that can locate veins in humans, Compared to the state of the art vein imaging; it has several characteristics [72].

4.2 Ear shape recognition

The use of ear imaging to identify people occurred more than 100 years ago. There are three methods of imaging the ear for identification: (a) taking a photograph, (b) taking marks, and (c) taking thermographic images of the ear. The essential parts of the ear for identification purposes correspond to the outer ear and the earlobe, but the structure and shape of the entire ear are also often necessary. Using the Image Ray Transform algorithm [74], a clear image of the outer ear can be systematically generated, this image is translated into a series of numbers for an identification process with a 99.6% success rate with several advantages such as (a) the ears are not affected by facial expressions (or the background), (b) the ears are consistent the age of the person, (c) ear imaging is non-invasive (can even be performed at long distance). However, some disadvantages include the transformation of the ears (with the use of jewelry or other accessories), the hair, the headphones, the lenses that cover the ears, the low light conditions, and the different angles of the ears images of ears.

Fig. 4 Biometrics educational trends
Some commercial applications, such as the biometric system based on recognizing the ear canal’s geometry to authenticate smartphone users with hearing aids, demonstrated efficiency of ~95% [7]. When a sound is played in someone’s ear, the sound is propagated and reflected and absorbed through the ear canal, all of which produce a unique signature that can be recorded with the microphone [21]. Other commercial systems indicate that they can distinguish between people based on their acoustic characteristics with an accuracy greater than 99% [47].

### 4.3 Facial thermography

Facial thermograms are unique to people and could devise methods and systems for identifying them. Thermograms show the amount of infrared energy emitted, transmitted, and reflected by objects. This infrared energy is converted into temperature, which offers an image with this temperature distribution [53]. Thus, thermography can function as a facial recognition system in which an infrared camera is used to capture the images. In addition, facial thermogram technology is more accurate and robust in different lighting and environmental conditions than video images, using bi-sensor data to uniquely and automatically identify people.

Thermograms are a non-intrusive human identification technology in which facial recognition using multispectral imaging modalities, such as IR imaging sensors, has become an area of growing interest. Thermal imaging can avoid some common facial recognition challenges based on video images, such as (a) face and skin detection, location and segmentation are more comfortable to perform, (b) within-class variation. Furthermore, it is less since they are not affected by external distortions, (c) invariance to changes in lighting and facial expressions, (d) works in total darkness, and (e) detects costumes (even though the person has makeup).

Additionally, electronic thermography is used more frequently as a non-ionizing and non-invasive alternative for medicine diagnosis [36]. The vascular heat emissions present on a person’s face can provide physiological indicators of the state of health or, where appropriate, the underlying disease.

### 4.4 Odor sensing

Identifying people through odors is not a new idea; Bloodhound dogs have been trained for years in this task, as body odor is a handy identifier. The primary odor contains stable components over time and does not change with food or the person’s environment, making it a successful biometric. A person’s secondary odor includes characteristics that are present due to dietary or environmental factors. Finally, the tertiary odor contains elements present due to external factors such as soaps and perfumes.

Real sensors have not yet reached the precision of a dog’s smell. Thanks to nano and biotechnology, there are still fundamental advances (thanks to nano and biotechnology) with high sensitivity to detect volatile elements in people’s body odor [37]. Even body odor can vary due to illness, food, mood swings, etc. These recognizable patterns in the body odor of each person have an identification error of 15%. This biometric technology is not intrusive, it works even with deodorants and perfumes since it is impossible to reproduce human’s smell. Electronic nose research groups have developed some prototypes of noses to smell different odors and aroma types [63], some have been successfully tested to search for people in risky situations such as earthquakes or other natural disasters. People can also be identified through their unique breath prints; This method is fast and non-invasive [43].

### 4.5 Gait recognition

Gait recognition is a behavioral biometric technology that identifies people based on their unique gait patterns. Minor variations in gait style can be used as a biometric identifier to identify individuals. Gait recognition correlates Spatio-temporal parameters such as stride length, stride width, gait speed, and cycle time with kinematic parameters such as joint rotation and the joint’s average angles, hip, knee and ankle, and the angles of the thigh, trunk, and foot; The length of the stride and the height of the person are also considered. Some research projects show 95% efficiency in identifying people [76].

There are important commercial applications that developed a gait recognition technique based on a smartphone’s information using a dynamic temporal distortion classification algorithm and an artificial neural network as an evaluation system to authenticate people [46]. Significant research investments have been generated to bring this image-based gait analysis to the market [44]. However, it is not the only case, several gait recognition systems have been developed, considering it an excellent biometric [6].

### 4.6 Heartbeat authentication

Heartbeat can not only detect humans, but it can also identify them. This is because the heartbeat follows an irregular pattern that never repeats and is unique to each person [3]. With an electrocardiograph (ECG), the unique mathematical features underlying this pattern can be extracted, and a secret key generated the system can use that to encrypt the information. Small changes in the initial conditions lead to very different results [12]. The shape of the heartbeat pattern is affected by several factors (size, shape, and heart position in the body).
The advantages of biometric information are: (a) it is difficult to clone a biometric marker or an ECG, (b) an ECG cannot be recorded without the permission of a person, and (c) it is non-invasive [66]. On the other hand, some disadvantages are (1) difficulty in capturing heartbeat patterns, (2) transformation with age or exercise response.

NASA has released a new patent for a heartbeat-based biometric system for commercial licenses to enable solution developers and integrators [72]. Besides, Huang et al. [31] strategically reuse ECG signals to improve data encryption, security level, and privacy.

### 4.7 Brain waves/activity

Using brain waves as an identifier is relatively new biometrics; it could serve as a security system and verify a person’s identity with less than 1% [1]. However, the noise associated with all the brain signal measurements has made data analysis difficult. Focusing on the waves in the brain area related to reading and word recognition produces a clearer signal that can be measured faster [30].

These brain signals are generated when people access their semantic memories, which record specific word’s meanings. This method could become a more personal and secure authentication alternative [39]. Additionally, scanned images of brain activity using functional magnetic resonance imaging can act as a signature pattern to accurately identify people. Some techniques measure neural activity through blood flow in the brain while people are awake and mentally active [65]. One advantage is that it is almost impossible to clone. The downsides are that the technology is intrusive and not easy to use because it is specialized equipment.

### 4.8 Human body bioacoustics

A modulated micro-vibration that travels through our body could capture a person’s unique spectral trait [49]. Sound waves passing through the human body can identify a person with 97% accuracy, analyze properties such as the individual’s skin, joint tension, and bone density [57]. The spectral patterns of bioacoustics do not undergo significant changes over time. Researchers used a transducer to generate vibrations and sound waves that pass through a person’s body. The finger is a part of the body that has been used to test this technique. Once sound passes through skin, bone, and other tissues, a sensor picks up the unique bioacoustic signature.

The biometric system can be very successful in identifying people; for example, different individual fingers can be identified. This means that a person must use the same finger used for authentication [27]. Auditory acoustics can also be used for authentication. The ear has unique characteristics that change from person to person [2].

### 4.9 Perceptual user interface

It is possible to use gestures to perform human–machine interaction with gesture recognition, a mathematical interpretation of human movements through a computational device. Currently, computing devices and smartphones have gesture recognition systems, games, and virtual reality systems, more interactive and immersive (i.e., Microsoft’s Kinect). These systems can also be used to authenticate a user [63].

Cheiloscopy is a forensic investigation technique that deals with the identification of humans from lip traces. Lip prints are unique and also permanent for every human being. Lip prints between family members (and between twins) generally revealed different patterns with few similar grooves suggesting inheritance in lip prints [70]. Cheiloscopy has mainly served forensics as an aid for personal identification; This technology has an enormous development [63].

### 4.10 New platforms

Biometric technology (as well as traditional systems) has been used mainly when the authentication or verification of the person occurs. However, new platforms are growing due to new demands and developing services. Mobile devices are growing, evolving, incorporating the latest technology platforms, and, with this, biometric systems are transforming and expanding. For example, Samsung’s Galaxy Tab has incorporated iris recognition technology to access the device. In addition, some portable devices, such as bracelets, measure the user’s heartbeat to authenticate purchases made with Mastercard credit cards on the site [22].

### 5 Conclusions

Biometric technology is relatively new and has changed the way identification and authentication processes are performed. It comprises innovative advances that measure the physical and behavioral characteristics of people. Biometrics is now used in various fields, including government, banking, healthcare, and education. The latter has reaped the benefits of biometric options to good effect. In addition, biometrics can be used to perform non-academic and academic activities at universities. Non-academic activities include the use of fingerprints to enter the campus or university dormitories, pay for a cafeteria or library service. Educational activities include monitoring student behavior or emotions to change teaching strategy on time, class attendance, taking electronic tests, analyzing motivations and progress in a course, and conducting learning analysis. However, some challenges need to be solved effectively, including user’s
reluctance to use technology. People may be afraid of how their personal information will be used.

As this is a new field of study, it could be challenging to provide students with the knowledge to develop such systems. In addition, privacy concerns are the primary concern, as devices can collect all kinds of personal information. Likewise, there is a need to improve biometric technology to make it more robust and develop more innovative solutions that solve society’s main problems or add value to the services offered, in this case, in the educational field.

An important aspect to consider is the choice of the appropriate biometric solution for educational institution’s needs. Some factors to consider are (Fry and Dunphy, nd): (a) choose a biometric identification system that can be used in multiple areas, that is, students are identified only once and have access to various services at the university (access to campus, cafeteria, classroom) attendance, library, etc.). (b) the biometric system must be scalable, that is, it must work well with a handful of students and increase their number, (c) the system must be compatible with the software that is already installed on campus, (d) before starting the system, make sure it works well; all traits of potential users need to be scanned, (e) consider accuracy and performance, (f) compare different providers, so that selection is based on an informed process, (g) communicate how the system works to all who will use it.

The biometric market is expected to reach $94 billion in 2025, at a compound annual growth rate of 36%, over the next 5 years. New features are being developed, such as vascular pattern recognition, ear shape recognition, facial thermography, odor detection, gait recognition, authentication of heartbeat, brain waves, and bioacoustics of the human body. The development of typical artificial intelligence algorithms combined with the technological growth of the Internet of Things (and its impact on Big Data) will be great catalysts for biometric systems to develop widely and impact many areas within them, including education. However, the biggest challenge for this technology to overcome is security and privacy concerns; they must be addressed to harness this technology’s full potential.

Finally, biometrics is a technology that can enhance students’ abilities in the context of Industry 4.0. Various interactive technologies fulfill this task. Such technologies are (a) 3D printing which enhances students understanding; (b) Augment reality which is an interactive technology that captures students attention; (c) Virtual Reality enhances students ability to connect theory and practice; (d) Cloud computing can be used to have access to the learning material from anywhere; (e) Holograms offer interactive spaces to learn [26]; (f) Artificial Intelligence permits students to have a better understanding of a given subject; (g) Robots capture students attention [67]; (h) Internet of Things allow students to be active learners [42].

Acknowledgements The authors would like to acknowledge the financial and technical support of Writing Lab, TecLabs, Tecnológico de Monterrey, México, in the production of this work.

References

1. Anthony, S.: No TitleBerkeley researchers replace passwords with pass thoughts by reading your mind. Retrieved April 15, 2020, from www.extremetech.com/computing/152827-berkeley-reseachers-authenticate-your-identity-with-just-your-brainwaves-replacing-passwords-with-passthoughts (2013)
2. Arakawa, T.: Ear acoustic authentication technology: using sound to identify the distinctive shape of the ear canal. Retrieved July 10, 2020, from www.nec.com/en/global/techrep/journal/g18/n02/180219.html (2018)
3. Aron, J.: Your heartbeat could keep your data safe. Retrieved April 15, 2020, from www.newscientist.com/article/mg21328516.500-your-heartbeat-could-keep-your-%0Adata-safe-%0A (2012)
4. Baird, S.: Biometrics “Security Technology”: it is important for students to understand that technology can be used as part of a solution to a problem. Technol. Teach. 61(5), 18–23 (2002)
5. Bowyer, K.W., Hollingsworth, K., Flynn, P.J.: Image understanding for Iris biometrics: a survey. Comput. Vis. Image Underst. 110, 281–307 (2008)
6. Burt, C.: Researchers unveil new AI gait recognition system. Retrieved from www.biometricupdate.com/201805/researchers-unveil-new-ai-gait-recognition-system (2018)
7. Burt, C.: Biometric ear canal geometry recognition developed by University of Buffalo Researchers. Retrieved April 15, 2020, from www.biometricupdate.com/201909/biometric-ear-canal-geometry-recognition-developed-by-university-of-buffalo-researchers (2019a)
8. Burt, C.: New technologies for finger vein, voice, and facial biometrics unveiled. Retrieved April 13, 2020, from www.biometricupdate.com/201908/new-technologies-for-finger-vein-voice-and-facial-biometrics-unveiled (2019b)
9. Burtte, C.: The Problem of Biometrics in Education. Biometric Technol. Today 2013(6), 5–7. Retrieved from www.sciedirect.com/science/article/abs/pii/S0969476513701115 (2013)
10. Caldwell, T.: Biometric tech has mixed fortunes in education. Biometric Technol. Today 3, 12 (2013)
11. Carlaw, S.: Impact on biometrics of Covid-19. Biometric Technol. Today 8–9 (2020)
12. Chen, C., Lin, C., Chang, C., Lin, S.: Personalized information encryption using ECG signals with chaotic functions. Inf. Sci. 193, 125–140 (2012)
13. Dafoulas, G.A., Maia, C.C., Clarke, J.S., Ali, A., Augusto, J.: Investigating the role of biometrics in education—the use of sensor data in collaborative learning. In: Int Conf e-Learning, pp. 115–123 (2018)
14. Dell Technologies Inc.: Gen Z is here. Are you ready? (2020)
15. Dinu, V.E., Papuc, D., Gheorghiu, A., Dascalu, M.: Biometric data in learning analytics: a survey on existing applications. In: The 13th Int Scientific Conf eLearning and Software for Education, pp. 465–473 (2017)
16. Dinu, V., Papuc, D., Gheorghiu, A., Dascalu, M. L., Moldoveanu, A., & Moldoveanu, F.: Biometric data in learning analytics: a survey on existing applications. In: 13th Int Scientific Conf eLearning and Software for Education, Bucharest, pp. 465–472 (2017)
17. Dwoskin, E., Rusli, E.M.: The technology that unmasks your hidden emotions. Wall Street Journal (Jan 28). Accessed Oct 20, 2020, from wsj.com/articles/startups-see-your-face-unmask-your-emotions-1424273298#:bLk8dH_DkLSJvA (2015)
18. Education Publishing Worldwide Ltd: Biometrics an option for schools wanting a secure future. Educ. J 280, 27 (2016)
19. Elliott, S.J., Peters, J.L., Rishel, T.J.: An introduction to biometrics technology: its place in technology education. J. Ind. Teach. Educ. 41(4), 1–8 (2004)
20. Ferguson, R.: Learning analytics: drivers, developments and challenges. Int. J. Technol. Enhanced Learn. 4(5/6), 304–317 (2012)
21. Gao, Y., Wang, W., Phoha, V., Sun, W., Jin, Z.: EarEcho. In: ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, p. 1 (2019)
22. German, R., Barber, K.S.: Current biometric adoption and trends. The University of Texas at Austin. Retrieved from identity.utexas.edu/assets/uploads/publications/Current-Biometric-Adoption-and-Trends.pdf (2017)
23. Gold, S.: Biometrics in education: integrating with the real world. Biometric Technol. Today 2010(4), 7–8. Retrieved from www.researchgate.net/publication/238294356_Biometrics_in_education_integrating_with_the_real_world (2010)
24. Gravemeyer, B., Mavrikis, M., Holmes, W., Gutierrez-Santos, Wiedmann, M., Rummel, N.: Affecting O-task behaviour: how affect-aware feedback can improve student learning. In: LAK, pp. 104–113 (2016)
25. Gray, S.L.: Biometrics in schools: the role of authentic and authentic social transactions. UCL Institute of Education. Retrieved from discovery.ucl.ac.uk/id/eprint/1545213/3/Leaton_Gray_Biometrics_BSA_conference.pdf (2017)
26. Halil, S.H.: Technological advancements in Education 4.0. Online J. Distance Educ. E-Learn. 7(1), 63–69 (2019)
27. Hampson, M.: The bioacoustic signatures of our bodies can reveal our identities. Retrieved July 10, 2020, from spectrum.ieee.org/the-human-os/telecom/security/the-bioacoustic-signatures-of-our-bodies-can-reveal-our-identities (2019)
28. Hidrogo, I., Zambrano, D., Hernandez-de-Menendez, M., & Morales-Menendez, R.: Mostla for engineering education: part 1 initial results. Int. J. Interact. Des. Manuf. https://doi.org/10.1007/s12008-020-00730-4 (2020)
29. Hoffman, F.: The effectiveness of biometrics in student education. Retrieved from www.n2sys.com/blog/guest-blog-posts/the-effectiveness-of-biometrics-in-student-education/ (2020)
30. Hond, B.: Your brain’s unique response to words can reveal your identity. Retrieved April 15, 2020, from www.newscientist.com/article/dn27555-your-brains-unique-response-to-words-can-reveal-your-identity/ (2015)
31. Huang, P., Li, B., Guo, L., Jin, Z., & Chen, Y.: A robust and reusable ECG-based authentication and data encryption scheme for eHealth systems. In: 2016 IEEE Global Comm Conf, pp. 1–6 (2016)
32. Jager, T.D.: Application of biometric fingerprinting to encourage the active involvement of student teachers in lectures on differentiated instruction. South Afr. J. Educ. 39(2), 1–11 (2019)
33. Jain, A., Ross, A., Prabhakar, S.: An introduction to biometric recognition. IEEE Trans. Circuits Syst. Video Technol. 14, 4–20 (2004)
34. Jraidi, C.M., Frasson, C.: A hierarchical probabilistic framework for recognizing learners’ interaction experience trends and emotions. In: Advances in Human–Computer Interaction (2014)
35. Kim, K.H., Bang, S.W., Kim, S.R.: Emotion recognition system using short-term monitoring of physiological signals. Med. Biol. Eng. Comput. 42(3), 419–427 (2004)
36. King, R.: Explainer: Facial Thermography. Retrieved April 15, 2020, from www.biometricupdate.com/201308/explainer-facial-thermography (2013)
37. Korotkaya, Z.: Biometric Person Authentication: Odor. Department of Information Technology, Laboratory of Applied Mathematics, Lappeenranta University of Technology (2003)
38. Krucoff, M.O., Rahimpour, S., Slutzky, M.W., Reggie, E.V., Turner, D.A.: Enhancing nervous system recovery through neurobiologics, neural interface training, and neurorehabilitation, neuroprosthetics. Front. Neurosci. 10, 584 (2016)
39. Lee, J.: Researcher says brainwaves could be a way for security systems to verify identity. Retrieved April 15, 2020, from http://www.biometricupdate.com/201505/researcher-says-brainwaves-could-be-a-way-for-security-systems-to-verify-identity (2015)
40. Levy, Y., Ramim, M.: A Theoretical Approach for Biometrics Authentication of E-exams. Nova Southeastern University, USA (2007)
41. Lynn, A.: Cyber Attacks History In Higher Education. Retrieved April 15, 2020, from www.informationsecuritybuzz.com/articles/cyber-attacks-history-in-higher-education/ (2018)
42. Maksimovic, M.: Facta universitatis, series: teaching, learning and teacher education. Facta Univ. Ser. Teach. Learn. Educ. 1(2), 137–150 (2018)
43. Martinez-Lozano, P., Kohler, M., Zenobi, R.: Human breath analysis may support the existence of individual metabolic phenotypes. PLoS ONE 8(4), e59909 (2018)
44. Mayhew, S.: Watrix Raises $14M, Releases Gait Recognition Solution. Retrieved April 15, 2020, from www.biometricupdate.com/201810/watrix-raises-14m-releases-gait-recognition-solution (2018)
45. Mordini, E., Tzovaras, D., & Ashton, H.: Introduction. In: Mordini, E., Tzovaras, D. (Eds.), Second generation biometrics: the ethical, legal and social context. The International Library of Ethics, Law and Technology, vol. 11, pp. 1–19. Dordrecht: Springer (2012)
46. Mufandaidza, M., Ramotsoela, T., Hancke, G.: Continuous user authentication in smartphones using gait analysis. In: 44th Annual Conf of the IEEE Industrial Electronics Society (2018)
47. NEC: NEC develops biometrics technology that uses sound to distinguish individually unique ear cavity shape. Retrieved April 15, 2020, from www.nec.com/en/press/201603/global_20160307_01.html (2016)
48. Nita, S., Mihailescu, M.: Proposing a secure e-learning system based on biometric authentication and homomorphic encryption. In: 14th Int Scientific Conf eLearning and Software for Education Bucharest, pp. 47–52 (2018)
49. Pascu, L.: Human body bioacoustics deliver 97 percent biometric accuracy, researchers say. Retrieved April 15, 2020, from www.biometricupdate.com/201911/human-body-bioacoustics-deliver-97-percent-biometric-accuracy-researchers-say (2019)
50. Pascu, L.: IGEL Integrates Fujitsu palm vein recognition to boost endpoint security. Retrieved April 13, 2020, from www.biometricupdate.com/202004/igel-integrates-fujitsu-palm-vein-recognition-to-boost-endpoint-security (2020)
51. Pato, J.N., Millett, L.L.: Biometric Recognition. Challenges and Opportunities. The National Academies Press. Retrieved from dataprivacylab.org/TIP/2011sept/Biometric.pdf (2010)
52. Pearson: Meeting the Expectations of Gen Z in Higher Education. Retrieved July 6, 2020, from www.pearson.com/us/content/dam/one-dot-com/one-dot-com/us/en/files/PSONA5646_8150_TIDL_GenZ_Infographic_Print_FINAL.pdf (2018)
53. Prokoski, F., Riedel, R.: Infrared identification of faces and body parts. In: Biometrics: Personal Identification in Networked Society. Springer, USA (1996)
54. Russell, J.A.: A circumpolar model of affect. J. Person. Soc. Psychol. 39(6), 1161–1178 (1980)
55. Salmeron-Majadas, S., Arevalillo-Herráez, M., Santos, O.C., Saneiro, M., Cabestrero, R., Quiros, P., Boticario, J.G.: Filtering of spontaneous and low intensity emotions in educational contexts. In: AIED, pp. 429–438 (2015)
56. Shimizu, K.: Optical trans-body imaging—feasibility of optical CT and functional imaging of living body. Med. Philos. 11, 620–629 (1992)
57. Sim, J., Noh, H., Goo, W., Kim, N., Chae, S., Ahn, C.: Identity recognition based on bioacoustics of human body. IEEE Trans Cybern 1–12 (2019)
58. Society of Learning Analytics: About. Retrieved July 6, 2020, from https://www.solaresearch.org/ (2020)
59. Šošević, U., Milenković, I., Milovanović, M., Minović, M.: Support platform for learning about multimodal biometrics. J. Univers. Comput. Sci. 19(11), 1684–1700 (2013)
60. Spalding, S.: Biometrics in tertiary education. Biometric Technol. Today 2011(5), 8–9 (2011)
61. Sutrop, M., Laas-Mikko, K.: From identity verification to behavior prediction: ethical implications of second generation biometrics. Rev. Policy Res. 29(1), 21–36 (2012)
62. Syed, S., Ali, B., Wan, W.: Technical issues and challenges of biometric applications as access control tools of information security. Int. J. Innov. Comput. Inf. Control 8(11), 7983–7999 (2012)
63. Thakkar, D.: Five Unconventional Biometrics that Surprisingly Exist! Retrieved April 15, 2020, from https://www.bayometric.com/5-unconventional-biometrics/ (2018)
64. Thales: Biometrics: authentication and identification (definition, trends, use cases, laws and latest news)—2020 review. Retrieved July 7, 2020, from https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics (2020)
65. The Conversation: Brain Activity is as Unique—and Identifying—as a Fingerprint. Retrieved April 15, 2020, from https://theconversation.com/brain-activity-is-as-unique-and-identifying-as-a-%0A fingerprint-48723%0A (2015)
66. The Economist: A Heart to my Key. Retrieved April 15, 2020, from http://www.economist.com/blogs/babbage/2013/05/biometrics (2013)
67. Timms, M.J.: Letting Artificial Intelligence in Education out of the Box: Educational Cobots and Smart Classrooms. Int. J. Artif. Intell. Educ. 26(2), 701–712 (2016)
68. Unar, J.A., Chaw, W., Abbasi, A.: A review of biometric technology along with trends and prospects. Pattern Recogn. 47(8), 2673–2688 (2014)
69. Venkatesh, R., David, M.: Cheiloscopy: an aid for personal identification. J Forensic Dent Sci. 3(2), 67–70 (2011)
70. Van Est, R.: Intimate Technology: The Battle For Our Body And Behaviour. Rathenau Instituut, The Hague (2014)
71. Verizon: 2019 Data Breach Investigations Report. Retrieved April 15, 2020, from https://enterprise.verizon.com/resources/reports/dbir/ (2019)
72. Vincent, B.: The Space Agency Announced Several Health and Biotech Technology Transfer Opportunities. Retrieved April 13, 2020, from https://www.nextgov.com/emerging-tech/2020/02/nasa-tech-could-replace-passwords-your-heartbeat/163292/ (2020)
73. Wampler, R., Klingler, S., Solenthaler, B., Schinazi, V.R., Gross, M.: Affective state prediction in a mobile setting using wearable biometric sensors and stylus. In: Proc of The 12th Int Conf on Educational Data Mining, pp. 198–207 (2019)
74. Yale Scientific: Ears: the new fingerprints? Retrieved April 13, 2020, from www.yalescientific.org/2011/05/ears-the-new-fingerprints/ (2011)
75. Yampolskiy, R.V., Ave, M.: Behavioural biometrics : a survey and classification. Int. J. Biometrics 1(1), 1–33 (2008)
76. Yang, K., Dou, Y., Lv, S., Zhang, F., Lv, Q.: Relative distance features for gait recognition with kinect. J. Vis. Commun. Image Represent. 39, 209–217 (2016)
77. Yang, L., Winters, K., Kizza, J.M.: Biometrics education with hands-on labs. In: Proc of the 46th Annual Southeast Regional Conference, pp. 18–23 (2008)

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