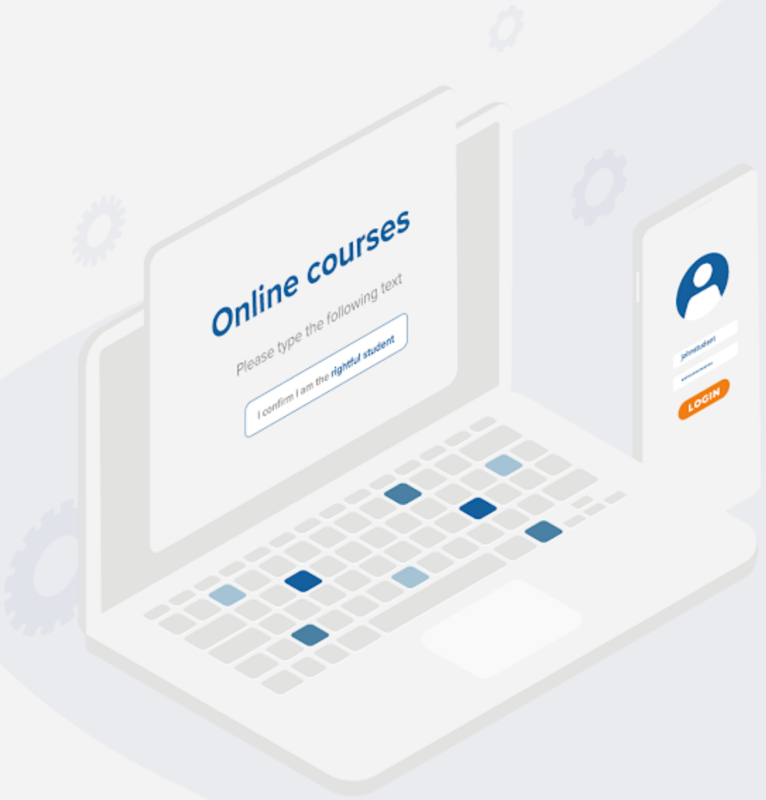

Online courses
Please type the following text
I confirm I am the rightful student
LOGIN

Student identity validation with keystroke dynamics

Content summary

1. **In the first part** of this document, we lay out the context of the recent incremental growth in online learning platforms usage for a better understanding of the need for adequate measures to verify remote learners' identities in today's fast-paced and technologically-enabled world.

2. **In the second** part we include more information on how identity verification and proctoring methods can prevent academic fraud and maintain the reputation of educational institutions.

3. **The third section** underlines the particularities of the most frequently used identity validation and proctoring factors in the field of online learning.

4. Finally, **the fourth section** focuses on TypingDNA's keystroke dynamics authentication product, an innovative behavioral biometrics technology which can be deployed for eLearning authentication and automated proctoring.

The context of the online learning environment

Who is studying online?

The discussion about the behaviors and preferences of different student groups in remote learning is highly relevant in the context of choosing the right identity validation methods—also known as authentication—which are often an integral part of robust proctoring systems.

The more familiar students are with technology, the easier it is to get them used to automatic proctoring and innovative, technology-based identity authentication alternatives.

A comparative analysis of online learning versus classroom learning shows that eLearning is especially effective for students who are confident in their ability to learn online, who are comfortable with technology, and who enjoy controlling the pace of the course.

Moreover, IBM has found that participants learn five times more material in online learning courses using multimedia content than in traditional classroom settings.

In the presentation "Engaging Generation Z students," Vickie Cook states that Gen Zers —those born after 1996— crave technology-enhanced learning opportunities.

This preference spurs from the innate tech-savvy particularity of their generation, as technology has always been a primary part of their lives.

Online learning is also appealing to millennials —those born between 1980 and 1996. Often called "digital natives", millennials are highly visual people who prefer "any time, any place" learning to traditional classrooms, according to an article from the University of Tampa.

Even though younger generations have fundamentally different behaviors than their predecessors, educational institutions have paid attention to their preference for remote learning and turned it into an opportunity to grow the eLearning industry.

The growth in online learning popularity and the growing need for remote proctoring

From K-12 to universities to continuous education platforms, learning providers all over the world are increasingly making their services available online.

In fact, the eLearning industry is projected to be worth $325 billion by 2025, partially due to the effort made by emerging economies to close the education gap but also due to digital transformation that's taking place across the world.

Latest update: The impact of COVID-19 pandemic on the eLearning industry

In 2020, online learning has become even more common with the emergence of the current pandemic of COVID-19, which is taking a toll on the entire world.

School closures have been made in over 50 countries around the world over the last month, in an attempt to slow the spread of the novel coronavirus, which has impacted the education of more than 1.5 billion children and youth.

With more than 91% of the world's total enrolled students being forced to stay at home, massive open online courses (MOOCs) such as Class Central, edX, Coursera and other online learning platforms have seen an unprecedented surge in usage.

For example, from February to March 2020, Class Central had a whopping 406% increase in the number of sessions while edX reached an impressive 19.2 million sessions with a 52% growth rate.

In a recent article, several teachers shared their thoughts on the explosion of remote learning and refer to the current situation as a "time of emergency adoption and experimentation that will speed up the adoption and embrace of online and other forms of technology-enabled learning."

The rapid transition schools were forced to make toward online learning will have a long-term impact. In the same article, one senior research associate said that "once colleges develop the capacity to serve their students via technology, there's little reason for them to abandon it."

However, proctoring requirements remain a key obstacle to the education industry's ability to transition online in such a short time. Many online services such as remote proctoring and student examination monitoring offer pricing strategies based on actual student use.

At the moment, due to the unprecedented number of students online, adopting such methods can overwhelm schools' budgets. It can also raise concerns with regards to the level of inclusiveness they provide across all students.

Before diving into a deeper discussion about the invigilation and authentication alternatives schools can choose from, it is important to get a better understanding of why these methods are required in the first place. To do that, we need to start with an overview of academic dishonesty as a primary threat to the integrity and reputations of educational institutions.

Traditional vs. automated proctoring to protect academic integrity

Creative cheating options are damaging the reputation of higher education and the overall integrity of degrees and certifications.

Believe it or not, more than **70% of all test takers admitted to having cheated at one point** in their academic careers. As such, making sure that the student doing the work is actually the one registered in the course is the first step institutions can take to lower the likelihood of rampant academic misconduct and dishonesty among students.

For both face-to-face and remote learning and examination programs, the introduction of proctoring and identity validation methods is crucial. Regardless of the cost and the changes that come with it, the remote invigilation market is estimated to reach **$10 billion by 2026**.

Identity validation

Both in-person and remote identity proofing can be done using webcams for facial recognition against student IDs such as passports or driving licenses. But it can also be done through the deployment of less intrusive technologies such as behavioral biometrics, which looks at the way students interact with their devices.

Identity proofing can be enacted at a course's registration level and also when a student enrolls to take an exam. It can also be enacted within courses and examinations to monitor students and to strengthen the institutions' ability to catch fraudsters and preserve the credibility of the assessment.

In-person versus remote proctoring

In-person human invigilators are required to ensure the security of an examination during face-to-face evaluations. But commercial testing centers are very expensive, and they take time to get to, which can inconvenience students.

Despite the prevalence of testing and live-proctoring centers such as Pearson and Prometic, where students complete exams under the close scrutiny of an invigilator, "**the advent of distance learning has made it impracticable to personally monitor each student taking an exam**".

As such, remote proctoring measures must be taken into consideration.

Remote proctoring is a form of exam invigilation which ensures the integrity of the examination by having an online exam invigilator or, better yet, **pairing human involvement with AI to catch fraudsters** and prevent students from cheating during quizzes, exams, and tests.

Many institutions that have transitioned their examinations online chose to replace test centers with remote live human-proctoring. But they were daunted by the huge operational and set-up costs, as well as the cost of **scaling third-party live human-proctoring service**.

Main challenges of traditional human proctoring in remote learning environments:

1. **Human error** can be found in both traditional face-to-face and online proctoring methods regardless of training, auditing, and oversight measures.
2. The inefficiency of human proctoring because the proctor has to watch a maximum of approximately **six to eight students simultaneously**.
3. **Scalability** is difficult for any organization, regardless of whether they serve thousands or millions of exams a year. Distributing proctoring responsibilities in an effective way requires an unsustainable and costly number of proctor-employees and work-hours to overcome examination volumes.
4. **Wait time** is associated with bad customer service, a challenge that includes the time a student spends connecting with a remote proctor, undergoing authentication, and proving they have a secure computing environment.
5. **Bandwidth**, **availability**, and **stability** are other major issues in online human proctoring.

Instead of diluting the course requirements by eliminating an exam or replacing them with projects or papers, institutions can use technology, AI, and automated proctoring systems to overcome the shortcomings of physical human-proctoring.

Benefits of automatic proctoring

1. **Robust and scalable** technologies broaden students' study options and make education more open, more accessible, and more flexible.
2. Automatic proctoring is **accessible and cost-effective** and provides a competitive advantage in the increasingly internationalized world of higher education. It’s an alternative option that meshes with today’s technology footprint.

What are the most frequently used identity validation factors?

Technology is innovating how we verify identities, allowing institutions to prevent academic dishonesty by introducing technologically enabled measures. Here are some of the more common ones.

Knowledge-based authentication

This category includes passwords, PIN codes, lock patterns, graphical passwords, and challenge questions. Knowledge-based authentication is the current predominant method used in eLearning.

Although students are accustomed to such methods, there is great vulnerability linked with passwords and personal questions, for example, which can be easily shared. Thus, passwords, PINs, and challenge questions alone provide less security and allow for higher levels of academic dishonesty.

Possession-based authentication

The identity verification process can be by asking students to present or apply physical objects such as a student ID card, driver's licence, personal ID, or token.

However, this type of authentication can often lead to student discontent and increased security costs for learning providers. Not only can these devices be easily lost or stolen, they are often inconvenient for students to carry along.

Biometric-based authentication

With biometric authentication, students can prove their identity based on their physiological and behavioral characteristics. **It can be argued** that biometrics is the most accurate, secure, and convenient authentication tool on the market because biometrics cannot be borrowed, stolen or forgotten, and replicating them takes a lot of effort.

However, certain physiological biometrics are hardware-intensive technologies. Fingerprint and facial recognition, for example, require expensive devices and are often intrusive for students.

But behavioral biometrics, including voice, gait, keystroke, signature, and mouse movement, are cost-effective and user-friendly, and require a much lower level of effort from students when proving their identities.

Category	Example	Advantages	Disadvantages
Knowledge	Password, PIN code, lock pattern, challenge questions	Effortless, popular, no cost	Can be passed on, forgotten, and hacked
Object	Physical tokens, smart cards, software tokens	Ease of use, low cost	Easily shared, lost, and stolen
Biometric	Fingerprint, facial recognition	Unique, unforgettable accurate	Costly, hardware required, invasive
Behavioral biometrics	Keystroke analysis, gait, mouse	User-friendly, secure, no hardware required	The AI's probabilistic outcome can lead to false negatives or false positives

Source: https://aip.scitation.org/doi/pdf/10.1063/1.5133925?download=true

Keystroke dynamics for students identity validation

Keystroke dynamics, also known as typing biometrics, is a behavioral biometrics tool that works by analyzing the unique rhythms and cadence of keypress events as students type a given phrase. The wide availability of keyboards ensures typing as the most accessible biometric on the market.

To give a real-world example of how the technology can be used, we can mention TypingDNA's typing biometrics authentication, which is currently **used by Improv traffic school to meet DMV requirements**, as well as **by UK's DVSA through Capgemini's implementation** to ease students' authentication in online driving tests.

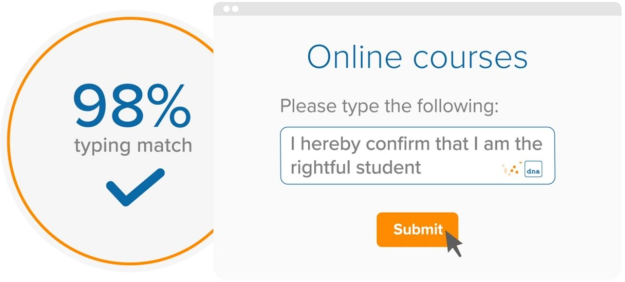
How is keystroke dynamics used in an eLearning scenario?

TypingDNA's typing biometrics can be used wherever the student types: during login when they type their user credentials or throughout exams and courses by typing a short text in a pop-in window to confirm their identity.

Registration and login identity validation

When a student types their user credentials during login, their typing pattern is matched with previously recorded samples.

If the match score released by the API is above a predetermined risk threshold—set by the educational institution—then the student is granted access to the learning environment.



Please type the following:

I hereby confirm that I am the rightful student

In-course or during exam proctoring

Throughout exams and courses, a pop-in window can appear at a determined or random time, prompting the student to type a short text to confirm their identity based on their typing pattern.

Why is keystroke dynamics a good fit for eLearning student authentication?

It’s accurate

Accuracy is one of the most important criteria in choosing the right authentication method. TypingDNA’s proprietary algorithms have reached an unprecedented accuracy in the industry of keystroke dynamics.

We always recommend that a student typing biometrics profile includes at least two enrollments, which are usually done during the registration phase for the course or exam by having the student type a short text to record their typing pattern.

Accuracy rises considerably when more patterns are added to a specific profile. In the case of strong typing biometrics profiles, typos and corrections do not pose a risk to accuracy. Instead, they are registered as particularities of a student’s behavior.

It’s accessible

For students, keystroke dynamics alleviates the stress of buying special hardware like webcam or fingerprint readers. It just requires a keyboard. It also works with low-bandwidth internet which allows students to access learning platforms from remote places.

It’s intuitive and non-intrusive

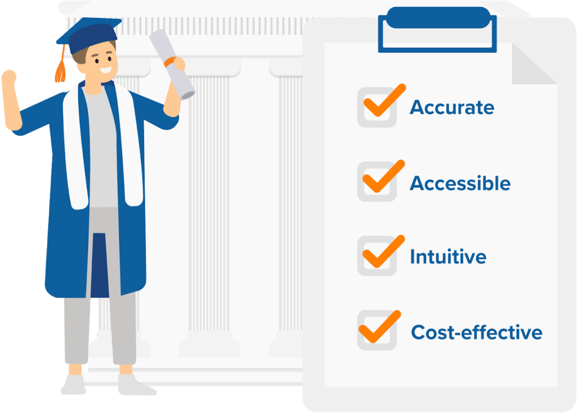
Typing biometrics works passively in the background without being intrusive to the students’ learning process. The undemanding and innovative nature of the typing-based authentication technology has proven to be a fun way for students to have their identities verified.

It’s cost-effective

For organizations, keystroke dynamics provide an opportunity to leverage AI and technology to ensure easily scalable authentication. It’s one solution that will work for everyone, because everyone’s typing patterns are unique—just like their fingerprints.

TypingDNA product overview

Learning providers can choose to use the same text or any text algorithms, depending on how they wish to authenticate their students, the scenario for the authentication, and the level of security they wish to impose.



Same text

Requires a smaller typing sample of around 20 to 30 characters to ensure accurate authentication. Users type the same text during enrollment as they do for identity verification.

Any text

The technology requires a longer typing sample—around 130 to 160 characters. The text users type during enrollment is different than what they type to verify their identities.

What if the user changes keyboards?

While there is a slight decrease in accuracy when a user changes keyboards (e.g., moving from a laptop to a smartphone), as long as the keyboards are similar, TypingDNA can authenticate students effectively.

What about false positives and false negatives?

Students type in many different ways either because passwords are difficult to remember or because they might type awkwardly at times. This variation can impact both false rejection and false acceptance rates.

A false rejection rate is defined as the measure of the likelihood that the biometric security system will incorrectly reject an authorized user's attempt to access the platform.

In an authentication scenario, a high false rejection rate (FRR) means rejecting the right user from accessing the course or exam. On the flipside, a high false acceptance rate (FAR) grants unauthorized access to a protected account, which is just as troublesome.

TypingDNA's algorithms can be adjusted to accommodate the security needs of the organization that deploys the technology, allowing clients to make informed and secure decisions based on their users' authentication scores.

To provide the desired authentication accuracy, we customized our offer of possible algorithms to optimize for user-friendliness and security.

1. **The best user experience** – using the lowest FRR provides a user-friendly process.
2. **The highest security** – the lowest FAR prevents fraud at the highest security level.
3. **A balanced approach** – delivering the best overall accuracy.

Our tests on the Same Text solution show that after the first three enrollments on up to 30 characters using a balanced approach algorithm—slightly dependent on the threshold set by the educational institution—our technology has a FAR of 3.98% and FRR of 4.39% with an accuracy of 95.82%.

It's worth noting that the accuracy increases and the FARs and FRRs go down once more enrollments are made.

If the user's typing pattern changes, can they still be authenticated?

To address slight but usual changes in typing behavior, new patterns can be stored on a user's profile. This way, there will always be an up-to-date "picture" of the user's typing behavior.

On rare occasions, the typing pattern of a user changes for good (e.g., permanent hand damage). In such a scenario, previously enrolled patterns have to be deleted, requiring a profile reset for the user in question.

There are situations when the typing behavior of a user changes temporarily—like when they break their hand, type on a different keyboard, or even have too much coffee to drink.

As typing biometrics is mostly used in the eLearning industry as a suspicious behavior flagging method, TypingDNA recommends that organizations use at least one additional security factor alongside typing biometrics, such as possession or knowledge-based measures (e.g., one-time passcodes or challenge questions).

How do we ensure users' privacy?

A typing pattern is an abstract numeric representation of typing behavior that can not be directly associated with the person who generated it. The user's identity stays with the customer, thus protecting their privacy.

How do we handle data?

Our clients include some of the largest global proctoring services, banks, and SaaS providers. To efficiently integrate our authentication products to serve millions of users, we offer flexible data storage options.

- Use our general cloud service for any authentication requests
- Use a private cloud dedicated server for a single client

Does it work on mobile?

Proprietary typing biometrics is available for native integrations on iOS, Android, and React Native. On mobile devices, our tests show higher accuracy based on the use of mobile sensor data in addition to keystroke times.

How can your institution start using typing biometrics authentication?

Check out our **education page** and get in touch with us by filling the form.