Solution Brief

Intel Security

Security in Education

AI and Confidential Computing help make secure remote exams a reality

Accessibility, Data Security, and Fraud Detection for Distance Learning

As an e-university where 80% of classes are delivered over the Internet, the Swiss Distance University of Applied Sciences (FFHS) takes online privacy and security very seriously. Even with more than twenty years of experience in distance learning, the University faces ongoing security challenges—and nowhere is that more serious than in the administration and evaluation of online exams.

FFHS has long provided some exams online, and the requirement to secure data while preventing cheating has always been important. In recent years, however, the need for comprehensive security became even more pressing as the COVID pandemic increased the demand for entirely remote learning. In addition, the complexity of online computing has also increased rapidly with advances in technologies such as artificial intelligence (AI), as well as the increasingly sophisticated threats to data integrity posed by criminal hacking and fraud.

To help meet the challenge of securing all aspects of the online exam process, FFHS joined forces with Intel Corporation to bolster the strength of their security capabilities in AI-based identity checking, fraud detection, and more.

Implementing Secure Exams

In preparation for this project, FFHS evaluated their previous examination system for two years. During that time, they identified a number of needs that could be met by a "virtual proctor" that would help detect and deal with fraud and cheating during exams. These needs included:

1. Significantly reduce the manual effort and hours required to monitor remote exams and to handle the massive amount of audio and video produced (more than 6.5 terabytes per semester).
2. Tie new functionality to the existing exam support system.
3. Protect exam data and students' privacy during remote examinations, complying with privacy and security laws like the EU General Data Protection Regulation (GDPR).

The initial approach to developing a digital system enabling secure remote exams was to implement an asynchronous analysis and evaluation process capable of recording video of students taking the exam. Because previous remote exams had demanded a significant effort by FFHS staff to monitor and evaluate, the new system would be designed to significantly reduce the human labor required.

Swiss Distance University of Applied Sciences, Brig, Switzerland

The Swiss Distance University of Applied Sciences (FFHS) delivers remote, online educational programs in disciplines such as IT, Engineering, Business, Communications, and more. Courses are tailored for continuing learners and learners who are unable to attend traditional classes on campus. Students can access courses on their own schedule, from anywhere in the world where connectivity is available. Fully accredited by the Swiss Accreditation Council, FFHS is a true e-university that provides all resources online, including course materials, virtual classrooms, interactive tools, and exams for bachelor's and master's degree programs. Having provided flexible, high-quality education for over 25 years, FFHS programs are well-respected and its graduates successful, with over 93% employed in work that matches their academic preparation.

*Source: Erudera.com, https://erudera.com/news/93-of-swiss-higher-education-graduates-get-employed-in-their-field-of-study-official-data-shows

To help achieve this, FFHS migrated the exam workload and models to Intel® DevCloud for the Edge, a cloud-based development platform that enables developers to create and test edge computing applications quickly.

FFHS began with student-identity-detection they had built with client API code in OpenCV and Python that had its own FaceID detection framework. Intel engineers worked with FFHS to transform the model into an advanced proctoring solution, using pre-trained models and libraries from the Intel® Distribution of OpenVINO™ notebook. This enabled intelligent, adaptive video analytics of captured exam footage (recorded via input from the student's PC camera and microphone).

The new system uses AI to analyze activities on screen, looking for behavioral patterns in the exam sessions that indicate possible fraud or cheating. Testing has shown a very high degree of accuracy in discriminating between "cheating" and "not cheating" activities. If suspicious activity is found, the system extracts relevant segments into an automatically created video of excerpts that can be checked later by a trained faculty member.

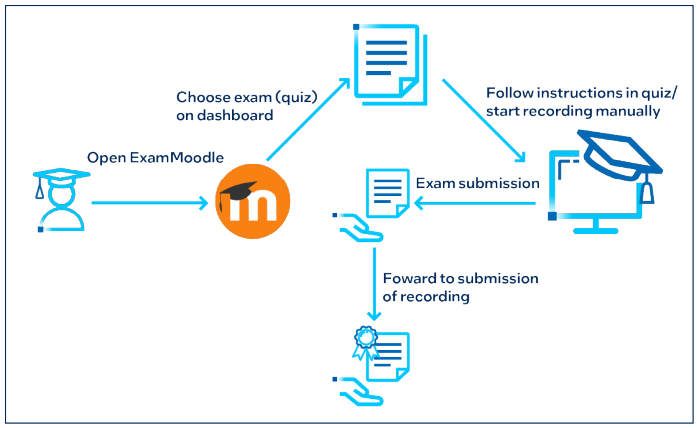

Figure 1. *Checking exams for suspicious activity*

Enabling Improved Student Support

To help maximize the new examination system's value, FFHS wanted to link to their existing telephone and ticket support services. This required enhancement through the addition of new channels to expand into a "live" support system. As mentioned earlier, an important objective was to improve on the previous system by automatically recording and saving examination videos for inspection by faculty members.

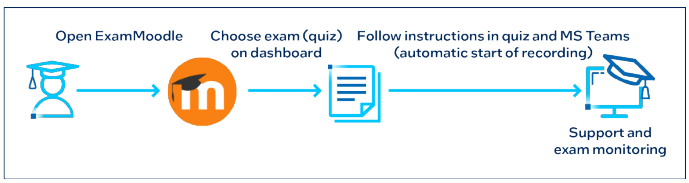

Figure 2. *Support and monitoring flow*

Confidential Computing in the Cloud

Protecting exam data and students' privacy during remote examinations was a core FFHS requirement. The secure exam platform relies on Confidential Computing to help protect data during processing, powered by Intel® Software Guard Extensions (Intel® SGX).

Implementing Confidential Computing with Intel SGX means access to sensitive data is limited during collection and processing. Available on 3rd and 4th generation Intel® Xeon® Scalable processors, Intel SGX is the most deployed and researched Trusted Execution Environment (TEE) for the data center, and it provides the smallest attack surface within the system. Intel SGX uses hardware isolation, encryption, and attestation to provide a high level of confidence in the integrity of the solution.

TEE isolation is designed to protect against intrusions from malicious actors or software, even if they have privileged system access. By protecting selected code and data from inspection or modification, developers can run sensitive data operations inside enclaves to help increase application security and protect data confidentiality.

Because the FFHS implementation relies on OpenVINO and other system resources for image processing, developers needed a standardized way to pass information between the TEE and OS services. FFHS achieved this using the open source Gramine Library OS. Gramine can run applications in an Intel SGX TEE with benefits comparable to running a complete OS in a virtual machine. This allowed developers to "lift and shift" existing OpenVINO webservice code into the appropriate Intel SGX enclave running on Azure Confidential Computing. Using this deployment approach enables cloud scaling and service availability.

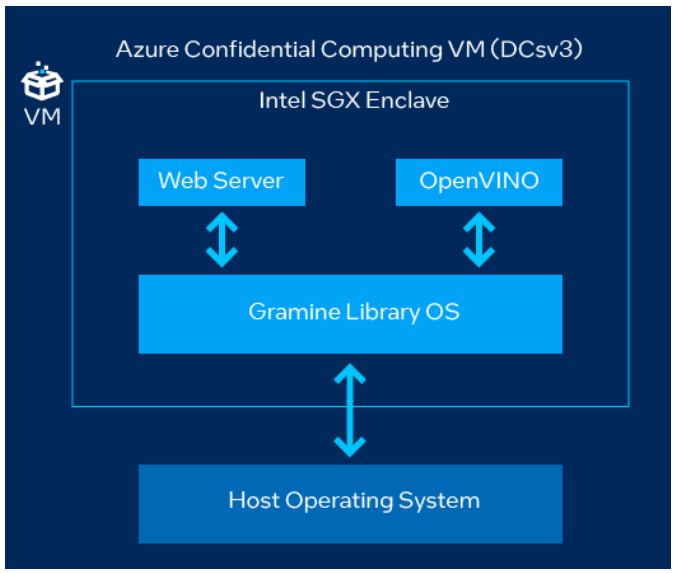

Figure 3. *Azure Confidential Computing*

Results

By integrating Intel SGX into sensitive areas of the new digital examination process (such as the AI-based identification of students during "Identity Check" and "Video Analysis"), FFHS can offer its students assurance that it is meeting state-of-the-art security standards during remote examinations. All system users—students, faculty, and staff—can be confident that both exam results and personal information are kept confidential and secure.

In addition, the new process saves a great deal of manual labor compared to the previous exam-checking system, with proctors or professors needing only two to four minutes per video, instead of one to two hours.[1]

As an added benefit, the optimized examination process will make it possible for students with disabilities to complete remote exams with fewer restrictions in the future, as accessibility considerations were taken into account throughout system optimization. FFHS consulted with experts in the field of accessibility to develop a special communication concept for live support.

FFHS intends to further enhance system functionality, add additional accessibility services, and package the online examination software as a product so educational systems can take advantage of a tested and proven Confidential Computing tool.

Learn more

The Swiss Distance University of Applied Sciences (FFHS)
https://www.ffhs.ch/en/

Intel® Xeon® Scalable processors
https://www.intel.com/content/www/us/en/products/details/processors/xeon/scalable.html

Intel Confidential Computing
https://www.intel.com/confidentialcomputing

Intel® Developer Cloud for the Edge
https://www.intel.com/content/www/us/en/developer/tools/devcloud/edge/overview.html

Intel® Distribution of OpenVINO™ Toolkit
https://www.intel.com/content/www/us/en/developer/tools/devcloud/edge/learn/openvino.html

Intel® OpenVINO™ Security Add-on
https://github.com/openvinotoolkit/security_addon/blob/master/docs/ovsa_get_started.md

Intel® OpenVINO™ Security Add-on for Gramine-SGX
https://github.com/openvinotoolkit/security_addon/blob/master/docs/ovsa_get_started_sgx.md

Gramine Library Operating System
https://gramineproject.io

Azure Confidential Computing
https://docs.microsoft.com/en-us/azure/confidential-computing/

1. Internal FFHS testing data.