

Best Practices in E-Assessments

with a Special Focus on Cheating Prevention

Dirk von Grünigen,
School of Engineering
Zurich University of Applied Sciences (ZHAW)
Zurich, Switzerland
vogr@zhaw.ch,

Fernando Benites de Azevedo e Souza
School of Engineering
Zurich University of Applied Sciences (ZHAW)
Zurich, Switzerland
benf@zhaw.ch

Beatrice Pradarelli
Polytech Montpellier/LIRMM/CNFM
University of Montpellier
Montpellier, France
beatrice.pradarelli@umontpellier.fr

Amani Magid
NYUAD Library
New York University Abu Dhabi
Abu Dhabi, United Arab Emirates
amani.magid@nyu.edu

Mark Cieliebak,
School of Engineering
Zurich University of Applied Sciences
(ZHAW)
Zurich, Switzerland
ciel@zhaw.ch,

Abstract—In this digital age of the computer, Internet, and social media and Internet of Things, e-assessments have become an accepted method to determine if students have learned materials presented in a course. With acceptance of this electronic means of assessing students, many questions arise about this method. What should be the format of e-assessment? What amount of time? What kinds of questions should be asked (multiple choice, short answer, etc.)? These are only a few of the many different questions. In addition, educators have always had to contend with the possibility that some students might cheat on an examination. It is widely known that students are often times more technologically savvy than their professors. So how does one prevent students from cheating on an e-assessment? Understandably, given the amount of information available on e-assessments and the variety of formats to choose from, choosing to administer e-assessments over paper-based assessments can lead to confusion on the part of the professor. This paper presents helpful guidance for lecturers who want to introduce e-assessments in their class, and it provides recommendations about the technical infrastructure to implement to avoid students cheating. It is based on literature review, on an international survey that gathers insights and experiences from lecturers who are using e-assessment in their class, and on technological evaluation of e-assessment infrastructure.

Keywords—*e-assessment, evaluation, competencies, technology, Moodle, grading, cheating*

I. INTRODUCTION

Almost all educators would like to believe that the material they have taught their students is actually *learned* by their students. But what is the best way to measure how much a student has learned? For hundreds of years, “testing” knowledge and skills was primarily surmised by giving the students an assessment or test, which was either a midterm examination or final examination. Although these assessments can take many forms, including oral exams or lab practical,

often it is in the form of a paper assessment, where tasks can be multiple choice, fill-in-the-blank, drawings, text answers, etc. With the advent of Information Technology (IT) and the Internet, assessments can also be given electronically.

Electronic assessment, also known as E-Assessment¹ (E-A), refers to evaluation methods and practices that emphasize the role of IT relative to measuring students’ learning.

Origins. The use of computer technology in educational assessment has a decades-long history. Computers were initially adopted for assessment in the 1970s in order to reduce human’s workload to mark examinations and rate scoring. Since then, assessment has progressed in conjunction with IT advancements and the arrival of the Internet in education. Nowadays, it is widely recognized that E-A can bring benefits at both administrative and pedagogical levels. As more and more learning activities run on Learning Management System (LMS) such as Moodle, both teachers and students get familiar to using such systems.

Building Blocks. For the purpose of this paper, we consider an “e-assessment” to be a summative examination in higher education in an engineering discipline (for an in-depth discussion of different conceptualizations of E-As, see [Guàrdia2016]). Implementing such exams includes four main building blocks, which we will discuss throughout this paper: general setup, exam content preparation, exam conduction, and exam grading.

¹ E-assessment can concern any type of examination: summative, formative or diagnostic. Many terms are related to e-assessment: online assessment, computer assisted/mediated assessment, computer -based assessment (CBA), computer-assisted assessment (CAA), computer-aided assessment (CAA), computer adaptive assessment (CAA), computer adaptive testing (CAT), online assessment, technology-enabled assessment, technology-enhanced assessment, technology-embedded assessments, technology-based assessment, Internet-based testing, web-based assessment.

Advantages. E-As have several obvious and well-known advantages, such as providing objective automatic grading, instant scoring and feedback, storage and reusability, and scalability [1]. In addition, assessments on computers offer the advantage to ease the reading of long text answers compared to handwriting papers, and IT solutions also allows for a wider range of tasks and activities that can enable teachers to evaluate their students in the appropriate environment for summative assessments. Finally, mobile and tablet devices provide new opportunities for formative E-A, like using clickers (audience/personal response systems) in large classroom environments.

Challenges. On the other hand, educators have several aspects to consider when moving to E-A, including: differences in preparation and conduction of the exam; prevention of cheating; changes in scoring schemes; and modified feedback mechanisms. Developing an online examination requires defining tasks that will allow to verify the student's skills in the appropriate context, and providing a technological setup and framework that is able to support the E-A (tools, network, and computers). It also requires the examiner to acquire the competencies to properly use digital tools and media and the LMS. In order to avoid technical issues during the conduction of an E-A, an IT hardware is required that can handle large numbers of student at the same time. One of the most important aspects is to prevent access of students to unallowed external help (humans) or resources (teaching material, internet) during the exam (cheating prevention) [2]. There exist several technical frameworks, such as Safe Exam Browser, that try to restrict and secure the computer's usage and reduce students' abilities to behave dishonestly during an E-A.

Guidance for Lecturers. At first sight, moving from paper-based exams to fully electronic assessments can appear to be a long journey. However, once E-As become more a routine, less (if any) technical preparation will be necessary for each individual examination.

II. LITERATURE OVERVIEW

There is an abundance of literature on the use of E-A in higher education. It has been successfully used in conjunction with flipped learning while teaching math students, resulting in higher pass rates and also favorable comments from students in the course [3]. However, one may argue that the manner in which students view taking online tests that can affect their use of it. In a survey of first year students studying STEM subjects, those who had a more positive attitude and found more enjoyment in online test were the ones who found E-A "useful" [4]. It is very common for many of the bigger publishers of university textbooks, to include online assessment modules as part of the textbook package. Upon surveying students of a class who used a textbook by Pearson publishers with a MyMathLab system, some of the customization features that students preferred were: multiple choice questions over true/false and single choice, at least 3 opportunities to retake the E-A, and the ability to allow for more time per question [5]. Online assessment modules are

also a common feature of Learning Management Systems. In conducting electronic assessments for 1st year engineering students enrolled in math classes, Moodle's psychometric analysis is able to measure the level of difficulty of questions, in addition to providing an excellent method of formative E-A [6].

Just requiring an E-A is not quite enough as the design of an E-A is important as well. Miller has shown that when presenting 2 types of E-A to university students studying American Sign Language, the E-A that took into consideration "aesthetic design" when it was constructed, was the one in which students felt compelled to finish the E-A, were happier and experienced "decreased cognitive load", that is the students were less distracted by other factors that have nothing to do with the assessment itself such as the design of the E-A and the willingness of the participant to continue based on the design [7]. In fact, incorporating aesthetics into the construction of an E-A has become a standard and crucial component [7-10].

Finding ways to prevent students from cheating on exams is always a top priority for professors who choose E-As. One group of researchers divided a class equally and exposed one group of students taking an E-A to a web based proctor, while the other group had no proctor. The students in the latter group felt there was more opportunity to cheat on the exam than the group that was monitored [11]. Dental students reported that using a privacy screen filter on a computer during the E-A made it difficult to read another student's screen [12]. A relatively simple way that students cheat during online exams is to have another student take the exam for them. Faculty at Taiwan University has found that implementing a notarization process, in which the students are required to take an exam at a computing lab on campus, and in which the computers are set up to take a photo of the student when they first sit down and during the time they are taking the exam, has greatly reduced the amount of cheating [13]. Setting up the computer to take a photo and/or video of the student taking an E-A has been in existence as early as 2004 [14].

III. SURVEY

We launched an international survey among university lecturers in order to gather insights and best practices for E-As. Despite wide distribution of the survey at several universities in different countries (more than 500 addresses), only 18 lecturers answered, most of them from Switzerland (11), followed by Germany (2), Australia (2), France (1), Greece (1) and South Africa (1). Participants were primarily masculine (88.2%), and most of them were between 35-45 years old (77%), with an equal distribution of ages below 35, between 46-55 and 56-65 years old (6.7% each).

The most important results are as follows:

- E-A concerns a wide range of fields: Applied Statistics, Language Translation, Electrical Engineering, English for Law, Programming and Digital Technologies, without any domain emerging significantly from the others.
- E-A is mainly implemented at the bachelor level. Regarding class size, it is almost equally used (around 20%) in classes

with 15-30 or 30-60 or 60-100 or 200-400 students.

- Multiple choice and short text answers are preferred to long text, calculation and yes/no answers.
- No auxiliary material is allowed in 50% of the E-As. When it is authorized, students can refer to other printed material, lecture notes, electronic notes, or they can open an Internet access to specific domains.
- Most participants used Moodle as LMS platform for E-A.
- Introducing E-As did not change the duration of the examination, which can be long (120 minutes), but it increased the preparation time and decreased the grading effort. The participants indicated that the main benefits of E-A (in decreasing priority) automatic grading of exams, statistics related to the exams outcomes, storing and reuse of exercises, and storing results (digital archive).
- In order to prevent technical difficulties, 69% of the participants provided spare machines and sometimes dedicated technical staff. In addition, 15% of them ran mock E-A.

One important and often-mentioned aspect was cheating prevention: Almost all participants implemented actions to prevent dishonest behavior of the students. Methods are relative to IT technology (such as no internet access, use of Safe-Exam-Browser, randomized questions, screen control), or relative to the environment (such as dedicated PC organization in the classroom that stops students' exchanges), or relative to the general circumstances (such as a strict time limitation and providing enough problems so that solving more tasks is more attractive than cheating). Participants generally agree that compared to pen-and-paper exams, E-As require more effort to avoid cheating, so it appears to be a major issue. Unlike E-A preparation, which efforts reduce with repeating exams practise, the efforts to prevent students' dishonest behavior appears to remain.

IV. REALIZATION OF E-ASSESSMENTS

In this section, we give an overview of scientific state-of-the-art, tools, resources and best practices for each of the building blocks for implementing an E-A - except for cheating prevention, which is described later on in a separate chapter due to its significance.

General Setup. The step of defining the general setup has the largest impact in the process, especially if E-As are conducted in a summative form as in the context of this study. Many conditions must be considered, among others the infrastructure, e.g. if there are enough institution computers or Bring Your Own Device (BYOD) must be required. Some universities provide special E-A rooms with over 100 work places (e.g. www.eassessment.uni-bremen.de) which offers a very stable setup, while others utilize "mobile" setups with computers or tablets [15]. Still, these choices can be constrained by money, space or human resources available, but also by factors identified within a risk analysis, such as "Denial-of-Service" attacks on the network, storage weaknesses, power shortage, computer problems, etc. On the other, the selected software framework should usually comply with following criteria: visual impression, ease of use, ease of

setup, short- and long-term costs, robustness, high-security standards. Often employed systems are LMS since they naturally continue electronic courses; most common are Moodle [16], ILIAS [17], and OLAT [18]. However, direct E-As system exists, e.g. DEWIS (dewis.uwe.ac.uk), Q-Exam (www.q-exam.net).

Also important are legal aspects, which can complicate and pose further conditions on the general setup. These conditions generally refer to aspects like security and duration of exam storages, legal appeal to e-exams because the used framework/setup, but also security (assurance of student identity) issues must be cleared.

These restraints can limit methods, although, for example in the exam content preparation, there is an explosion of methods that can be used, as audio, video, virtual reality, simulation, drawing, programming tasks, additional material as open book or even the internet, enabling students much more possibilities than with paper and pen. When the physical and software setup is defined and the legal context is cleared, a carefully exam preparation is due.

Exam Content. Each exam should be designed with a theoretical background on didactics, considering different aspects such as: competency assessment, learning goals, exam objectivity, and taxonomy of educational objectives [19]. Further, providing access to a computer enables, as indicated above, a variety of other media, increasing the input and possibilities of an exam, thus allowing students multiple (sensorial) access to the content.

Thus, this additional material or media can have a pedagogical impact as well or even be necessary; just as interpreters, who render one language into another orally in real time, need audio samples to perform. Software studios enable the students to solve more difficult problems in a period of time, which might fit within an E-A, especially with regards to simulation, programming and mathematics. However, typical question types for E-As are still technically very simple: free text (short or long), hotspot, drag and drop (graphical or text), analogy questions, selection list, causality questions, multiple choice (table, multiple, single), answer pairs.

Exam Conduction. The examiners and exam conductors must be instructed into the framework and trained or briefed for technical problems, especially if additional media/software is involved. An obvious solution would be to offer the exam as paper, but that is problematic when using media; still some students might prefer a paper solution [20]. Further, additional computers, as backup, can usually be only made available in a certain contingent.

Nonetheless, another point of view on the examination should be taken into consideration: "many students cited the usefulness of mock e-exams" [21]. Such mock e-exams help the students to familiarize with the system and adjust the expectations on the tests (from both sides, students as lecturers).

Exam Grading. The last step is grading. There is an expectation on saving time and costs but also having more freedom and at the same time objectivity. The freedom

regarding location (home-office) and different possibilities to marking, especially, to achieve objectivity more easily through semi/automatic grading. Furthermore, data mining methods can give more insights about the course, such as on student performance (as for example the language in free-text answers can be analyzed), but also highlights more easily the difficulties in the exam (e.g. readability of the questions).

Since multiple questions are easy to automate, they are very often employed and provided by many frameworks in multiple variations. However, it is a controversial question type. Usually, the more degree of freedom of the answer the more difficult it is to mark it, especially when automating. Already for semi-structured questions, as filling the blanks or numeric values in mathematical questions, the answers must be normalized. This is a laborious task (finding synonyms, formatting numbers: $0.35=3.5E-1$, etc.), and can be very difficult to solve. Interestingly, there are some approaches for semi-automatic grading, where similar answers are grouped together, pursuing same marking quality [22], and even approaches of automatic grading on free-text answering using deep learning [23]. Although, machine learning and artificial intelligence can provide more objectivity in grading, there are a myriad of examples where these technologies, when applied autonomously, failed and therefore are not widespread.

For programming courses, there are in principle two ways to test the results for correctness: black-box or white-box testing. Whereas, black-box testing with input-output – e.g. as performed by a variety of Moodle’s plugins (e.g. vpl.dis.ulpgc.es) - poses a very specific expectation on the result of the student’s program, missing a measurable value for how much a solution is wrong, depriving a student of a valuable input. In turn, white-box testing is a difficult task, and in combination of code style can be compared to written essay examination, where not only result but the way it is written becomes a central point in the evaluation.

However, a critical aspect must be also considering while designing all these steps: academic dishonesty and measures to prevent it.

V. CHEATING PREVENTION IN E-ASSESSMENTS

Classical Cheating. There are numerous ways of cheating in an exam: first, there are the “classical” ways, such as talking to a neighbour, passing a note around, cheat sheets and many more. All of these ways to cheat can - and should - be prevented in the same way as in pen-and-paper exams, e.g. by an attentive supervisor, sufficient space between student tables etc. But using electronic devices for conducting assessments introduce new potential ways to cheat. Most of these rely on accessing the Internet.

Cheating with Internet Access. If students have access to the internet, they have access to unlimited sources of information, such as encyclopedic websites such as Wikipedia or WolframAlpha, textbooks (e.g. Google Books) or research articles (e.g. Springer Link or ResearchGate), but also Question-Answering websites such as Yahoo Clever (answers.yahoo.com), Quora (quora.com) or StackOverflow

(stackoverflow.com).

However, Internet access also introduces the problem of communication with others while taking the exam, which is even more severe, because communicating with others is usually strictly prohibited. Internet connectivity enables exactly that: students can communicate with each other through messaging channels (e.g. E-Mail, WhatsApp); they might seek help via Q&A websites such as Quora or StackOverflow; or they can even communicate with dedicated external experts, which allows them to “outsource” the solving of their exam. In an extreme case, one could imagine that a student simply sends, say, the PDF of the exam tasks to an expert, which then in turn solves it and sends the solutions back to the student.

Finally, network connectivity also allows for direct access to the students’ computer, for instance via shared screens or remote desktop access, e.g. with TeamViewer (www.teamviewer.coI). Here, a third person can read and fill out the entire exam directly via the student’s computer.

Technical Devices. There are two different ways how E-As can be conducted with respect to the devices used (typically computers or tablets): first, the traditional approach is to use devices provided by the institution where the exam is conducted (institutional devices). In such a setup, cheating is a problem and must be tackled by implementing technical and organizational measures, but most of the potential attacks can be limited or mitigated because the devices are managed by the institution itself. This allows to ensure that, for example, no prohibited software is installed, there is no or only restricted internet access, and monitoring software can track potential modifications of the basic system setting.

Cheating also has to be prevented when using institutional devices. But the main difference in using such devices instead of the students’ devices is that they are managed by the institution. Hence, most of the potential attacks against the system cannot be easily performed because the students do not have access to the devices before the exams start. For this reason, we are mainly going to discuss measures which can be used to prevent cheating in “Bring Your Own Device (BYOD)” approaches.

The second type is BYOD scenarios: In this case the students work on their own devices. This is usually the same device as they have used throughout the semester. This implies that the students have all of the resources they gathered in a certain course (e.g. scripts, exercises) available on their device, if desired. This is usually not a problem in an open-book assessment, but it already poses an issue if the exam is supposed to be closed-book. But, even more fundamental problems arise when internet access has to be restricted or forbidden, since the examiner does not have full control over the installed software on the devices.

In the following paragraphs we will discuss two technical measures that may help to mitigate these issues. These measures are applicable with both BYOD and exams taken on institutional devices. However, we will focus more on the BYOD case, since enforcing policies on personal devices is usually more difficult than on institutional devices because of

the lack of control and oversight.

Lock-Down Software. The first solution we consider is a so-called "lock-down" or "kiosk" software. This is a special application, which, when started, locks down the device. This means that only the lock-down software is run and the user, or in this case the student, has no access to any other resource on the device (unless explicitly allowed). This allows to do a closed-book exam in a BYOD setup, where the institution does not have full control of the devices.

Lock-Down Browsers. The most common lock-down software comes in the form of lock-down web-browser. In most situations, such a lockdown browser is then used in combination with an LMS, such as Moodle or OLAT, where the students take their E-As. One example of such software is the "Safe Exam Browser" (SEB) [24] developed at the ETH Zurich, which was specifically developed for E-As. Most of the time, the SEB or similar software is used in E-As conducted on institutional devices [25,26], and it has already successfully been used in such settings at different universities. However, we evaluate SEB in the context of BYOD setups, where such a lock-down software would be installed on the devices of the students to control their access to additional resources (e.g. files, internet, ...). There is more similar software on the market, such as the QuestBase Secure Browser (www.questbase.com/product/qsb) or the SoftwareSecure Secure Exam Browser (www.softwaresecure.com/product/secureexam-browser). They provide features similar to the SEB, but are proprietary rather than open source as SEB.

Security Analysis. Sogaard offers an extensive technical security analysis of the SEB in [27]. In the following, we summarize the major issues with this approach. It will turn out that a lock-down software raises the effort that is required to cheat, but it is not the one-for-all solution for securing E-As in BYOD setups, especially with tech-savvy students.

Restricted Access to Resources. The SEB allows the lecturer to create a specific configuration for an E-A, where the lecturer can specify various different parameters, such as the following:

- Software which the student is allowed/disallowed to use
- Black-/Whitelists for URLs to visit with the browser
- Specific password for quitting the lockdown application

Using these configurations, the lecturer can control which resources are available and accessible on the computer during the exam - as long as the SEB is running and active.

Exiting the Lock-Down Software. An important part of a lock-down browser is the disabling of possibly "harmful" system commands to exit it. For example, on devices with the Windows operating system, keyboard commands, such as CTRL+ALT+Del (locking the device) or ALT+Tab (switching applications) must be disabled. This ensures that the student cannot exit the lock-down mode without either knowing the exit password or restarting its device. But here also lies one of the main problems, which most lock-down browsers have in common: If one restarts the device, the lockdown browser will

not automatically restart itself after start-up. Hence, students who are struggling in an E-A may be tempted to restart their device for getting access to the other resources available on their device. Even though this is easily noticeable by an attentive supervisor, it is still a problem when an E-A with several hundred students is taken, since having oversight for all of them either requires an extensive number of supervisors.

Operating System Coverage. Most lock-down systems are only available for Windows and Mac, but not for Linux-based operating systems. This poses another problem, especially in computer science courses, where many students are using Linux. In fact, in the case of lock-down browsers we are not aware of any product, which provides this functionality for Linux systems.

Other Vulnerabilities. Lock-down browsers also may have other problems. For instance, for the SEB we identified the following two potential vulnerabilities: One can control a system where SEB is running on a Windows machine from remote via the "Remote Desktop Protocol". This allows third persons to view and even act on the student's screen. SEB's source code is publicly available via GitHub. This leads to a problem because tech-savvy student can download the code, modify it (e.g. disable security-features) and build its own version. This problem also applies to closed-source software to some degree, but modifications are much more easily applied in open-source software.

Screen and Physical Recording. Another way to prevent cheating in a BYOD setup is to simply record the screens of students' devices and store these recordings. They can then be used to check whether the student has cheated, in case any suspicion arises. There are two main ways on how to record the screen of students: Either via software or via physical cameras.

Software Recordings. In order to record the screens of the students, they have to install a recording software on their devices. Popular examples of such software are the Open Broadcaster Software (OBS, <https://obsproject.com>), or ObserveIT (www.observeit.com). When the exam starts, the students start to stream the content of their screens to a specified backend server in the network. This brings the benefit that the students can be monitored while the exam is conducted, and the screen contents can be evaluated on the fly, which potentially allows to detect dishonest behavior early. The backend server then stores these streams in the form of videos, which the lecturer can look at later.

Required Resources and Other issues. Software recording sounds simple and promising at first sight; however, there are several potential issues which arise: First and foremost, the approach only works if the network is stable, otherwise the stream does not make it to the backend server and, hence, no video is recorded. The bandwidth required for a large number of students streaming simultaneously must not be underestimated: A preliminary test using the mentioned OBS client with an nginx Server (<https://nginx.org>) as the backend showed that streaming a video with a resolution of 720p and 5 frames per second on 200 devices requires around

400-500 gigabytes of storage (and corresponding network bandwidth).

Further, a major issue is that an actual backend service has to be implemented and maintained, which leads to additional costs. In additions, tech-savvy students might be able to circumvent such a software recording technology, for example by streaming a pre-recorded video instead of their actual screen content, running it inside a virtual machine. In principle, there are countermeasures for each of these attacks, but similar to the lock-down software, there is no total security.

Finally, one major issue is related to privacy. Depending on the country, it is prohibited to record the activities of students on their computer during the exam. This depends on the privacy laws of the country and has to be clarified before setting up the exam.

Physical Cameras. The basic setup is straightforward: simply distribute the required number of cameras throughout the room where the E-A is taken, so that all students and their devices are filmed from behind. The main benefits of this solution over the direct recording of screen via software is that it is much less vulnerable to technical problems or attacks, such as network connection drops or problems with installing the software on the students' devices.

Main Issues. The main problem of physical cameras is that it cannot be guaranteed that the screens are always recorded, because the students may sit in different positions while taking the exam, which can lead to their bodies blocking the line of sight between the camera and the screen. In addition, similar to screen recordings there are privacy issues to consider, which are even more severe in this setting, since the cameras do not only record the exams itself, but also the students in person.

VI. CONCLUSION

The science of e-assessments is a rapidly changing field, with new methods and technologies in development. Although there was not a large sample size, the survey results coincide with what exists in the literature, particularly that students prefer multiple choice and short text, that professors prefer e-assessment as it decreases time spent grading, and that professors take measures to decrease any academic dishonesty that could potentially take place during the e-assessment.

We have described the main building blocks of e-assessments, and gathered resources and best practices for implementing them. The results presented in this paper are the

outcome of a "Smart Teaching"-project, which aims to collect inspiring and innovative ideas for teaching at the university level. A more detailed discussion will be published at <http://dreamboxx.com/SmartTeaching>.

One major issue in e-assessments is cheating prevention, since access to the Internet allows for new ways of dishonest

behavior in comparison to pen-and-paper exams. Preventing cheating requires extensive technical and organizational measures in any case. We have analysed several technical measures such as screen recording or lock-down browsers to prevent cheating when the exam is conducted on the students' computers. Each of these approaches has its own set of vulnerabilities and drawbacks, which allow students to possibly circumvent the preventive measures.

The best solution at present is, in our opinion, a combination of several technologies, such as combining a lock-down browser with recordings by physical cameras. The lock-down browser drastically raises the amount of effort a student must exert in order to cheat, while the cameras are a strong threat that cheating might even be detected after the exam.

REFERENCES

- [1] L. Moccozet, O. Benkacem, P.-Y. Burgi, "Towards a technology-enhanced assessment service in Higher Education," presented at the 19th Interactive Collaborative Learning, 2016.
- [2] L. Guardia, G. Crisp, "Trends and challenges of e-assessment to enhance student learning in Higher Education," in *Innovative practices for higher education assessment and measurement*. IGI Global, 2016, pp. 36-56.
- [3] K. Henderson, "Using e-assessment to support flipped-style teaching," *MSOR Connections*, 15(2), pp. 34-41, 2016.
- [4] E. Acosta-Gonzaga, N. R. Walet, "The role of attitudinal factors in mathematical on-line assessments: a study of undergraduate STEM students," 03/07/2016.
- [5] Y.-W. Sek, C.-Y. Law, T.-H. Liew, S. Bt Hisham, S.-H. Lau, A. N. B. C. Pee, "E-Assessment as a Self-Test Quiz Tool: The Setting Features and Formative Use," *Procedia - Social and Behavioral Sciences*, 65, 2012, pp. 737-742.
- [6] M. Blanco, M. Ginovart, "On How Moodle Quizzes Can Contribute to the Formative e-Assessment of First-Year Engineering Students in Mathematics Courses," (in English), *RUSC*, 9(1), pp. 354-370, 2012.
- [7] C. Miller, "Aesthetics and e-assessment: the interplay of emotional design and learner performance," *Distance Education*, 32(3), pp. 307- 337, 2011.
- [8] B. Wilson, "Broadening Our Foundation For Instructional Design: Four Pillars Of Practice," *Educational Technology*, 45(2), pp. 10-15, 2005.
- [9] P. Parrish, "Embracing the aesthetics of Instructional Design," *Educational Technology*, 45(2), pp. 16-24, 2005.
- [10] N. Tractinsky, A. Katz, D. Ilkar, "What is beautiful is usable," *Interacting with Computers*, 13, pp. 127-145, 2000.
- [11] K. Hylton, Y. Levy, L. P. Dringus, "Utilizing webcam-based proctoring to deter misconduct in online exams," *Computers & Education*, vol. 92-93, pp. 53-63, 2016.
- [12] M. P. Escudier, E. W. Odell, J. A. Tricio, "Student Acceptability of High-Stakes e-Assessment in Dental Education: Using Privacy Screen Filters to Control Cheating," *JOURNAL OF DENTAL EDUCATION*, 78(4), pp. 558-566, 2014.
- [13] L. I-Fan, C. Ruey-Shin, L. Hao-Chun, "An Exploration into Improving Examinees' Acceptance of Participation in an Online Exam," (in English), *Journal of Educational Technology & Society*, 18(2), pp. 153-165, 2015.
- [14] C. C. Ko, C. D. Cheng, "Secure Internet examination system based on video monitoring," *Internet Research*, 14(1), pp. 48-61, 2004.
- [15] Universität Basel. (2016, November 20). Erste elektronische Prüfung auf iPads an der Medizinischen Fakultät. Available: www.unibas.ch/
- [16] M. Dougiamas, P. C. Taylor, "Moodle: Using Learning Communities to Create an Open Source Course Management System," presented at the EdMEDIA, 2003.
- [17] M. Kunkel, *Das offizielle ILIAS 4-Praxisbuch: Gemeinsam online*

lernen, arbeiten und kommunizieren. Deutschland GmbH: Pearson, 2011, ISBN:9783827329639.

- [18] S. Arnold, J. Fisler, "OLAT: the swiss open source learning management system.," presented at the e-Education, e-Business, e-Management, e-Learning, Sanya, China, 2010.
- [19] L. W. Anderson, D. R. Krathwohl, A Taxonomy for Learning, Teaching, Assessing. A Revision of Bloom's Taxonomy of Educational Objectives. 2001, p. 336.
- [20] H. Schulz. (2016, November 20). Studenten schreiben an Uni Siegen Jura-Klausur am Laptop statt auf Papier. Available: www.wp.de/
- [21] S. Wibowo, "A pilot study of an electronic exam system at an Australian University," *Journal of Educational Technology Systems* 45(1), pp. 5-33, 2016.
- [22] N. Escudeiro, P. Escudeiro, A. Cruz, "Semi-Automatic Grading of Students' Answers Written in Free Text," *Electronic Journal of e-Learning*, 9(1), pp. 15-22, 2011.
- [23] S. Zhao, Y. Zhang, X. Xiong, A. Botelho, N. Heffernan, "A Memory-Augmented Neural Model for Automated Grading," presented at the Proceedings of the 4th ACM Conference on Learning @ Scale (L@S '17), 2017.
- [24] D. R. Schneider, B. Volk, M. Lehre, D. Bauer, T. Piend, "Der Safe Exam Browser. Innovative Software zur Umsetzung von Online- Prüfungen an der ETH Zürich. ," in *Digitale Medien-Werkzeuge für exzellente Forschung und Lehre*, 2012, pp. 431-441.
- [25] T. Halbherr, N. Dittmann-Domenichini, T. Piendl, C. Schlienger, "Authentische, kompetenzorientierte Online-Prüfungen an der ETH Zürich," *Zeitschrift für Hochschulentwicklung*, 11(2), pp. 247-269, 2016.
- [26] A. K. Adesemowo, H. Johannes, S. Goldstone, K. Terblanche, "The experience of introducing secure e-assessment in a South African university first-year foundational ICT networking course.," *Africa Education Review*, 13(1), pp. 67-86, 2016.
- [27] T. M. Sogaard, "Mitigation of Cheating Threats in Digital BYOD exams" Master's Degree, Computer Science, Norwegian University of Science and Technology, 2016.
- [28] B. Küppers, F. Kerber, U. Meyer, U. Schroeder, "Beyond Lockdown: Towards Reliable e-Assessment," in *Bildungsräume 2017, Gesellschaft für Informatik*, pp. 191-196.