British Journal of Educational Technology Vol 50 No 2 2019 861–875
doi:10.1111/bjet.12608

e-Authentication for online assessment: A mixed-method study

Alexandra Okada, Denise Whitelock, Wayne Holmes and Chris Edwards

Alexandra Okada is a research fellow on technology-enhanced learning in the Open University UK's Institute of Educational Technology (OUUK-IET) and an honorary lecturer on Responsible Research and Innovation at the Open University in Brazil and Portugal. Denise Whitelock is a professor of Technology-enhanced Assessment in the OUUK-IET, with over 20 years of experience in designing, researching and evaluating online learning in Higher Education. Wayne Holmes is a lecturer in the OUUK-IET and has been involved in educational technologies for more than 25 years. Chris Edwards is a lecturer in the OUUK-IET and chairs the Masters module "Openness and innovation in e-learning." Address for correspondence: Dr Alexandra Okada, The Open University, IET, Walton Hall, MK76AA Milton Keynes, United Kingdom. Email: ale.okada@open.ac.uk

Abstract

Authenticating the students' identity and authenticity of their work is increasingly important to reduce academic malpractices and for quality assurance purposes in Education. There is a growing body of research about technological innovations to combat cheating and plagiarism. However, the literature is very limited on the impact of e-authentication systems across distinctive end-users because it is not a widespread practice at the moment. A considerable gap is to understand whether the use of e-authentication systems would increase trust on e-assessment, and to extend, whether students' acceptance would vary across gender, age and previous experiences. This study aims to shed light on this area by examining the attitudes and experiences of 328 students who used an authentication system known as *adaptive trust-based e-assessment system for learning (TeSLA)*. Evidence from mixed-method analysis suggests a broadly positive acceptance of these e-authentication technologies by distance education students. However, significant differences in the students' responses indicated, for instance, that men were less concerned about providing personal data than women; middle-aged participants were more aware of the nuances of cheating and plagiarism; while younger students were more likely to reject e-authentication, considerably due to data privacy and security and students with disabilities due to concerns about their special needs.

Introduction

European research on the impact of policies for plagiarism in higher education highlighted an increasing level of student plagiarism and cheating (Bermingham, Watson, & Jones, 2010; IPPHEAE, 2013; Park, 2004; QAA, 2016). The amount of plagiarism and cheating in high-stakes assessments has increased with the introduction of e-assessments (Harmon & Lambrinos, 2008; Underwood & Szabo, 2003). This means that the authentication of student digital identities has become especially important for reducing cheating in online distance education (Chew, Ding, & Rowell, 2015).

Cheating in online assessments has been examined at various levels. For example, Harmon and Lambrinos' study (2008) investigated whether online examinations are an invitation to cheat and found that more mature students who have their direct experience or working with

Practitioner Notes

What is already known about this topic

- The use of online assessments has raised concerns over malpractices.
- e-Authentication systems are emerging for detecting plagiarism and cheating.
- The literature about e-authentication systems in higher education is under-explored.

What this paper adds

- An e-authentication system framework with functionalities to check identity and authorship.
- Knowledge about the acceptance of e-authentication across students' genders and age groups.
- A model for evaluating trust-based e-authentication system.

Implications for practice and/or policy

- Students' needs should be considered when designing e-assessment tasks with e-authentication.
- e-Authentication might be more effective and perceived as more trust-worthy when combining different instruments.
- System feedback on data privacy and e-authentication outcomes should be provided to end-users to increase trust.

academics are less likely to cheat. This group were also found to be more open to e-authentication systems, believing that they will assure the quality of the online assessment and will contribute to a satisfactory assessment experience. Meanwhile, Underwood and Szabo (2003) highlight an interrelationship between gender, frequency of internet usage and maturity of students, and an individuals' willingness to commit academic offences. Their study, which focused on UK students, found that new undergraduates are more likely to cheat and plagiarise than students in later years of their degree. Finally, here, Okada, Mendonca, and Scott (2015) stressed that reliable examinations, credible technologies and authentic assessments are key issues for quality assurance (reducing cheating) in formative and summative assessments.

Students can easily cheat on the internet by texting answers, cutting-pasting ideas without attribution or purchasing professionally written essays and claim as their own original work. One way of addressing this problem is the use of new technologies and promote more *authentic* assessments as advocated (Whitelock, 2011). This paper builds on technology-enhanced assessment by focusing on the findings from a pilot study undertaken by The Open University UK (OUUK) as part of the EU-funded *Adaptive Trust-based e-Assessment System for Learning* (*TeSLA*) (http://tesla-project.eu). The *TeSLA* system was designed to check student authentication and authorship through a combination of the following instruments:

- **Biometrics**: facial recognition (analysing the face and facial expressions), voice recognition (analysing audio structures) and keystroke analysis (analysing how the user uses the keyboard).
- **Textual analysis**: anti-plagiarism (using text matching to detect similarities between documents) and forensic (to verify the authorship of written documents).
- **Security**: digital signature (to authenticate) and timestamp (to identify when an event is recorded by the computer).

Our investigation is based upon the Responsible Research and Innovation (RRI) approach, which implies that researchers, end-user and technologists interact during the whole process of research and innovation to better align both its process and outcomes with the values, needs and expectations of society (EC, 2016). Through RRI society and innovators become mutually responsive to each other with a view on the ethical acceptability, sustainability and societal desirability of the innovation process (Von Schomberg, 2011). This RRI study examines student perceptions of cheating and their disposition to provide personal data when requested for e-authentication. Such findings will be of interest for e-authentication technology developers, online distance educational institutions and policy makers.

e-Authentication systems and instruments

There is a growing body of literature focusing on the security and validity of online assessment supported by technology. In particular, various studies have recommended that online distance universities use traditional proctored exams for high-stakes and summative purposes (Edling, 2000; Hanna, 1998; Harmon, Lambrinos, & Buffolino, 2010). However, this recommendation, while understandable from an organisational and authentication point of view, brings self-evident difficulties. For example, those who have mobility difficulties, those who are in full-time employment and those who live at a considerable distance, having to attend an examination centre in person can be especially challenging (Hanna, 1998). Other recent studies (Apampa, Wills, & Argles, 2010; Harmon *et al*., 2010) have focused on commercial e-authentication systems (Table 1) that have been adopted by several universities.

Apampa *et al*. (2010) argue that e-assessment systems are perceived as secure and appropriate when the instruments successfully identify (*Who are you?*) and authenticate (*Is it really you?*) the examinee. Karim and Shukur (2016) draw attention to four groups of instruments for online authentication, which they term: *knowledge*, *biometric*, *possession* and *others*. To this, we add a fifth group: *learning output based on the e-authentication instruments offered by* the *TeSLA* project (see Figure 1).

- **Knowledge**: authentication is based on the students' knowledge of private information (eg, name, password, security question). Advantages of *knowledge group tools* include that they can be easy-to-use and inexpensive, while disadvantages include that they provide low-levels of security because they rely on knowledge that is susceptible to collusion and impersonation (Ullah, Xiao, Barker, & Lilley, 2014).
- **Biometrics**: authentication is based on physiological and behavioural characteristics. Physiological characteristics include facial images (2D or 3D), facial thermography, fingerprints, hand geometry, palm prints, hand IR thermograms, eye iris and retina, ear, skin, dental and DNA. Behavioural characteristics include voice, gait, signature, mouse movement, keystroke and pulse (Gao, 2012). Advantages of *biometric group tools* include that they can be effective and accurate, while disadvantages include that they can be technically complex and expensive (Levy & Ramin, 2007).
- **Possession**: authentication is based on private objects that the examinee has in their possession, such as memory cards, dongles and keys (Hastings & Dodson, 2004). This tends to be the least popular e-authentication group of instruments, mainly because they can be stolen or copied by other examinees.
- **Other**: authentication is based on a *process*, such as the examinee's location, a timestamp or their IP address.
- **Learning output**: authentication is based on what the student has written and how the writing has been structured, eg, by means of anti-plagiarism software and forensic textual analysis.

Table 1: e-Authentication systems—adapted by Okada from Karim & Shukur (2016)

		Biometrics			
Systems	*Knowledge*	*Behavioural*	*Psychological*	*Other*	*Learning output*
Remote Proctor	–	–	Fingerprint	–	–
ProctorU	Username, password, ID photo	–	–	Human proctor, Audio-video monitoring	–
ProctorCam	Username, password, ID photo	–	–	Human proctor, Audio-video monitoring	–
Kryterion	–	Keystroke rhythms	Face-recognition	Secure browser, Video monitoring	–
BioSig-ID	Username, password	Signature	–	–	–
ProctorFree	Username, password	–	Face-recognition	Secure browse	–
TeSLA	Username, password	Voice recognition, Keystroke analysis	Face-recognition	Timestamp	Anti-plagiarism, Forensic analysis

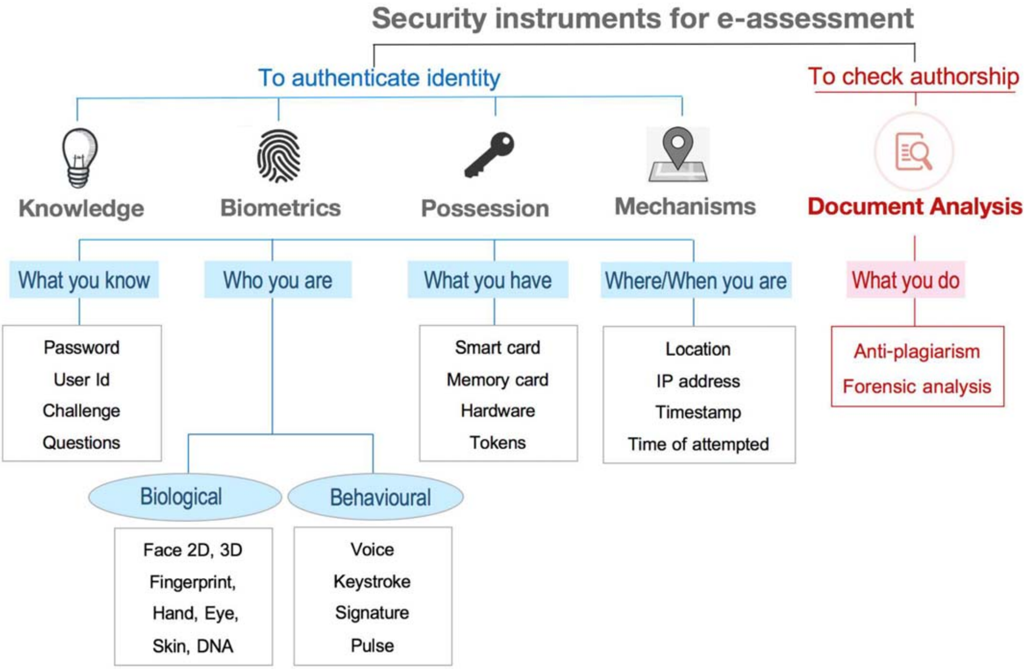

Figure 1: e-Authentication instruments framework for online assessment [Colour figure can be viewed at wileyonlinelibrary.com]

Research questions

To understand the various issues raised above and to contribute to the refinement of the *TeSLA* e-authentication tools, we investigated student attitudes to e-assessment with e-authentication utilizing the following research questions:

- How aware are students about cheating and plagiarism in online assessments?
- Do students consider e-authentication to be a practical, secure, reliable and acceptable alternative to traditional face-to-face (proctored) assessments?
- Do gender, age and previous experience with e-assessment have an impact on e-authentication?

Methodology

The *TeSLA* project conducted a number of empirical studies between February and June 2017 involving seven universities across Europe: Anadolu University, University of Jyväskylä, Open University of the Netherlands, The Open University UK, Sofia University, Technical University of Sofia and the Open University of Catalunya. They received local ethics committee approval and all of the data were anonymized. It aimed to check the efficacy of the *TeSLA* instruments while gathering feedback from users about their experiences using the instruments. The *TeSLA* instruments piloted by the OUUK were keystroke analysis and anti-plagiarism, chosen because of their relatively straightforward implementation in a Moodle virtual learning environment. A mix methods model was used to triangulate statistical and qualitative findings on student performance, views and concerns.

Participants

The OUUK invited 13 227 undergraduate students from different online courses by emails. The students were allocated randomly to either the keystroke analysis tool or the anti-plagiarism tool.

A total of 648 participants completed the pilot. This paper analyses a selection of data from the 328 participants who also answered both the pre- and post-questionnaire.

This students-sample was broadly comparable with overall OU student demographics (Jelfs & Richardson, 2013). It comprised 41% male and 59% female participants. Thirty percent of the sample were aged up to 30 years old ("young-students"), 26% were between 31 and 40 years old and 23% were between 41 and 50 years old ("middle-aged") and 23% were more than 51 years old ("senior-age"). Approximately 8% were students full time, 66% employed students, 7% were retired, 6% were not working and 13% had other activities. Additionally, 28% completed vocational, 24% secondary school, 13% bachelor's degree, 9% master's degree, 27% other and 26% disabled. Finally, 39% of the sample had previous experience of e-assessment, while 61% consider that did not.

Procedures

The participants were free to drop out of the study anytime. They were asked to complete the following steps in the *TeSLA* Moodle environment:

1. **Log in**: access the system with their OU username and password.
2. **Consent form**: read and sign a 1-page document that presents data protection and privacy information about their participation in *TeSLA* project.
3. **Pre-questionnaire**: complete a 20-question questionnaire about their previous experience with e-assessment, their views on plagiarism and cheating, their views on trust and e-authentication and their willingness to share personal data for e-authentication.
4. **Enrolment task**: complete an activity to initialise (set a baseline for) the system. This involved the participant typing 500 characters for keystroke analysis. There was no enrolment task for the anti-plagiarism instrument.
5. **Assessment task**: complete a task that involved typing answers to some simple questions (anti-plagiarism instrument) and upload a previously assessed module assignment (keystroke analysis).
6. **Post-questionnaire**: complete a 15-question post-questionnaire about their experience with the *TeSLA* system, their opinions of e-authentication systems, their views on trust and e-authentication and their willingness to share personal data.
7. **Focus group or Interview**: attend 40 minutes session on Skype to provide detailed views (selected participants only)

Data collection and analysis tools

The quantitative data analysed in this study was drawn from the pre-study and post-study questionnaires. The responses were converted into variables with binary values and imported into the (Cohesive Hierarchical Implicative Classification) CHIC tool, which was used to generate dendrogram visualisations for cluster analysis. The clusters are based on a similarity index to compare objects and variables based on likelihood connections, which enables researchers to extract association patterns from data (Gras & Kuntz, 2008; Lerman, 2016).

Findings

Descriptive statistical analysis

A descriptive statistical analysis was used to answer the first and second research questions about students' views on e-authentication, and on the viability of using e-authentication in lieu of traditional proctored assessments. The options strongly agree and agree were combined as well as disagree.

Participants' awareness on cheating and plagiarism

They were asked whether they agreed or disagreed that *it is plagiarism if I help or work together with a classmate in an individual activity and the work we submit is similar or identical* (Table 2). Most

Table 2: Students' awareness on cheating and plagiarism

Categories	*Variables*	*Values*	*Pre-survey*	
Awareness	It is plagiarism if I help or work together with a classmate in an individual activity and the work we submit is similar or identical	Agree	256	78%
		Neutral	26	8%
		Disagree	46	14%
	It is cheating if I copy-paste information from a website in a work developed by me without citing the original source	Agree	311	95%
		Neutral	3	1%
		Disagree	14	4%

participants agreed (78%), while much smaller percentages were not sure (8%) or disagreed (14%). Participants also appeared to be aware of some aspects of "cheating" in e-assessments. Participants were asked whether they agreed or not with the statement *it is cheating if I copy-paste information from a website in a work developed by me without citing the original source*. An overwhelming number of students agreed (95%), while only very small percentages were unsure (4%) or disagreed (1%).

Participants' opinions on e-authentication

Pre-questionnaire and post-questionnaire answers were very similar (Table 3). First, participants were asked whether or not they agreed that "the university is working to ensure the quality of the assessment process." In both the pre-questionnaire and post-questionnaire, most agreed (91% and 90% respectively), while small numbers of students were either unsure (7%, 8%) or disagreed (2%, 1%). The participants were also asked whether "they would trust an assessment system, in which all assessment occurs online." Again, the difference between pre-questionnaire and post-questionnaire was very small. Most participants agreed (77% and 79% respectively), while smaller numbers were either unsure (13%, 12%) or disagreed (10%, 9%). Finally, participants were asked whether they agreed or disagreed with the statement "the use of security measures for assessment purposes makes you feel that the university does not trust you." On both questionnaires, only a small number of students agreed with this statement (5%) while most disagreed (95%).

Table 3: Students' acceptance or rejection of e-authentication systems

Categories	*Variables*	*Values*	*Pre-survey*		*Post-survey*	
Acceptance	e-Authentication & quality	Agree	296	90%	297	91%
	Trust online assessment	Agree	254	77%	259	79%
	University does NOT trust students	Disagree	311	95%	311	95%
	Personal data: willing to share in order to be assessed online	Video of my face	103	31%	0*	0*
		Still picture of my face	223	68%	0*	0*
		Voice recording	195	59%	0*	0*
		Keystroke dynamic	210	64%	235	71%
Rejection potential issues	e-Authentication & quality	Disagree	8	2%	4	1%
	Trust online assessment	Disagree	32	10%	28	9%
	University does NOT trust students	Agree	15	4%	15	4%
	Personal data: willing to share in order to be assessed online	None	18	0.05	29	0.09

*Video, picture and voice recognition were not tested.

Table 4: Students' opinions about e-authentication

Categories	*Variables*	*Values*	*Pre-survey*	*Post-survey*
Practical issues	I am satisfied with the assessment	Agree	251	77%
		Disagree	77	23%
	The workload is greater than I expected	Agree	95	29%
		Disagree	233	71%
	I felt an increased level of surveillance	Agree	48	15%
		Disagree	280	85%
	I felt more stressed	Agree	33	10%
		Disagree	295	90%
Security and Reliability	My personal data was treated in a secure way	Agree	253	77%
		Disagree	75	23%
	I received technical guidance	Agree	106	32%
		Disagree	222	68%
	Issues were quickly and satisfactorily solved	Agree	60	57%
		Disagree	16	15%

Students' disposition to submit personal data for e-authentication

Participants were asked about which types of personal data they were willing to share as part of an e-authentication process (Table 3). Only 16% were willing to share all the types of personal data that they were asked about and only 31% were willing to share video. However, 68% of participants were willing to share their photograph and 59% were willing to share a voice recording. In addition, after participating in this study, 64% were willing to share their keystrokes and 69% were willing to share a piece of their written work.

Participants' opinions on practical issues with e-authentication

After their involvement in the *TeSLA* study, participants were asked whether they were "satisfied with the assessment"; most participants agreed (77%) (Table 4).

They were also asked whether "the workload is greater than I expected," whether they "felt an increased level of surveillance due to the TeSLA pilot," and whether they "felt more stressed when taking assessments due to the use of security." Most participants disagreed with each of these statements (71%, 85% and 90% respectively). Finally, participants were asked questions about security and reliability. Most (77%) agreed that their "personal data was treated in a secure way." However, while 68% disagreed that they had "received technical guidance," 57% of respondents agreed that "issues were quickly and satisfactory solved."

Statistical cluster analysis

Impact of gender

Figure 2 shows an extract of the various indexes of similarity (IoS) between the variables generated by the CHIC software. Data indicate a high similarity between female participants and those who said that they did not receive technical guidance (IoS = 0.768) when using the *TeSLA* system; and a high similarity between male participants and those who were willing to share personal data: voice and video recordings (0.997) and photographs (0.953). Male participants also had a smaller but noteworthy similarity (0.401) with those who are willing to share keystrokes after using the *TeSLA* system. The similarity tree shown in Figure 2 suggests that participants aged over 51 years who are retired and have completed masters-level education have limited previous experience of online assessment (0.850). Finally, here, the full similarity tree shows a high similarity between senior women who were more than 50 years old and retired

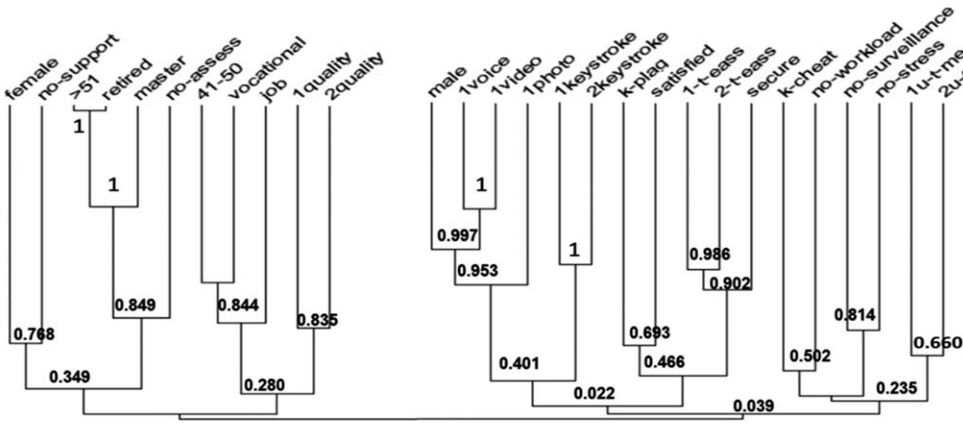

Figure 2: Cluster analysis about the effect of e-authentication by gender

participants, who hold a master degree and middle age (from 41 to 50) who have a full-time job and a vocational qualification with those who have not previously experienced an online module with online assessments.

Trust and security

Figure 2 also suggests two clusters related to plagiarism and cheating. The first cluster includes participants who are aware of what constitutes plagiarism and those who were satisfied with the online experience (0.693). The second cluster includes those participants who expressed trust in online assessments and those who believe that their personal data are treated in a secure way (0.902). Further, these two clusters have a smaller but noteworthy connection with each other (0.466). Finally, those participants who do not "feel an increased level of surveillance" are linked to those who do not feel more stressed when taking assessments due to the use of security procedures (0.814), and to those who have trust in their institution (0.661).

Impact of age group

The similarity tree analysis also suggested other noteworthy clusters (Figure 3). A first such cluster includes young students (<22 years old), all of whom had previous experience with online assessment (1.00), with those who requested technical guidance and had all their technical issues solved (0.897). A second cluster includes young students (22–30 years old) who were strongly linked (0.996) with those who disagreed that e-authentication will improve the quality of e-assessment

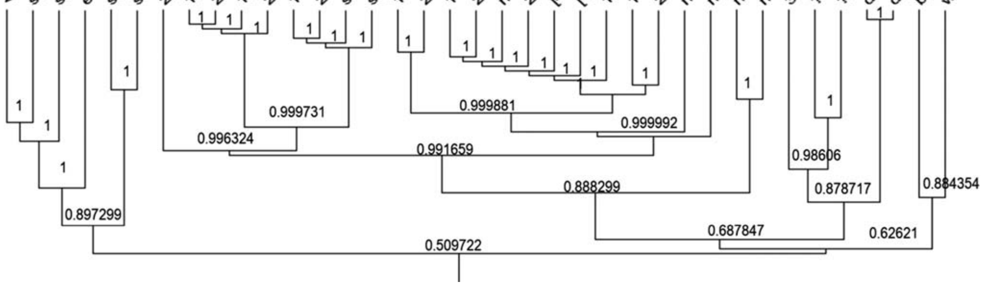

Figure 3: Cluster analysis about the effect of e-authentication by age-group

systems. This group were also strongly linked (1.00) with those who agreed that universities using e-authentication did not trust them, those who felt more stressed and those who felt an increased level of surveillance (1.00). They were also strongly linked (0.991) with those who were unsure about trust or security and did not want to share their personal data, those who were not satisfied with the assessment experience and did not have their technical issues solved, and those (0.882) who did not agree with the examples provided about plagiarism and cheating. A third cluster includes middle-aged students (31 to 40 years old) who were strongly linked with those who were unsure about the examples provided on plagiarism and cheating (0.986) with special educational needs (0.878) and not satisfied with the assessment experience (0.687). A fourth cluster includes students who hold a bachelor's degree who were strongly linked with those who indicated that the e-authentication system had a higher workload than expected (0.884).

Qualitative data analysis

To examine the views of students, qualitative data were gathered via emails, focus group and phone interviews with a template of topics defined by the *TeSLA* team. Based on thematic analysis of students' opinions with NVivo software tool, five features emerged related to a "trust" based e-authentication system as following described.

1. **The system will not fail or be compromised** (see Extract 1):

   One of the most frequent concerns among young students who were *not satisfied with the assessment* in the post-questionnaire, refers to technical problems that they faced, and time spent longer than expected.

Extract 1: Students' concerns on technical issues

> I was quite happy to undertake the survey but after completing the 2nd half, the system just cleared the screens and I received a response saying I'd not completed it. I couldn't be bothered to type it all again (student 1, woman, 22–30 years old)
> The server rejected my POST request saying the upload was too large. The PDF file was 318 KB. (student 3, man, 22–30 years old)

2. **The system is secure and data is private and safe** (see Extract 2):

   Students were also concerned about data privacy, cyber security and functional safety. They shared various questions about personal data stored in their computer and about spy attacks and unauthorised access. These learners would also like to be more informed

Extract 2: Students' concerns on privacy, security and safety

> I use my personal computer for studying, software development, online shopping, social media, internet banking and gaming… I want to know if this is a snooping software, and if it is, what justifies that? (student 4, man, 22–30 years old group)
> I would like to know how is the data sent? (What protocol is used?) Is the data transmission secure? (Is the data sent encrypted using TLS/SSL using a reasonably secure key?) . . . (student 5, man, 22–30 years old group)
> Are there plans to enforce the use of TeSLA? (will I be forced to use this regardless of my privacy concerns? (student 6, man, 22–30 years old group)
> How do I know if my data was kept safely in the system (such as facial and voice recording) Who can access my personal data? (student 9, woman, 31- 40 years old group)

about the e-authentication procedure including the special needs group who presented their concerns about trust.

3. **No adverse impact on learning and assessment experience** (see Extract 3):

   Students also presented worries about the outcomes of the system, particularly with the accuracy of the authentication. Their concerns included questions about what they should do if the system does not recognise their identity and authenticity. They also mentioned that they would like to receive responsive feedback from the system while they were using authentication.

Extract 3: Students' concerns on e-authentication issues that might impact on assessment

> How do I know if the system recognised me successfully (who I am, what I do)? If not then what shall I do? Do I have to provide my photo and video? What shall I do if the system does not recognise my face? (student 8, female, 31 to 40 years old group).
>
> What will happen if the system does not recognise me? Will it offer an alternative? Will this affect my time of assessment or my learning experience? (student 10, woman, 22–30 years old group)
>
> i have a very distinctive typing style and i do type a little slower than normal students and pause a lot but i had no problems with the system… The only major concern i would have is … if the TeSLA crashes and you lose half of what you have been typing and you have say 30 minutes to retype things so that is something that must be considered. (student 11, woman, special needs group)

4. **The system will not affect performance** (see Extract 4):

   Various issues were also raised by students who were worried if the e-authentication process would affect their performance. For instance, students revealed some concerns about the requirements for keystroke dynamics such as typing flow and speed. Additionally, participants of the special needs group were not confident to use e-authentication instruments. For instance, a student with dyslexia mentioned that she needs more time and breaks to complete their work and her writing during keystroke dynamics will be different to her assignment.

Extract 4: Students' concerns on e-authentication issues that might impact on their performance

> … people might start wondering if the typing flow and speed is significant and it is easy to get distracted by trying to type fast. (student11, man, 31–40 years old group)
>
> E-authentication, as an OU home-based student is very important especially as I am a disabled student, however, … this requires my confidence in internet security and with all authentication in any of the processes regarding my online study. (student 7, woman, special educational needs, special needs group)
>
> My writing and grammar is simplistic and my spelling is awful. Its just how my dyslexia works… That is my major concern because i wouldn't want it to come to a point where the OU would be looking at my assignments and then looking at my exam and thinking, there is something wrong here because the difference between the two and causing a lot of stress… I need at least 25% more time and i also have to take breaks so there would have to be pauses in the exam. (student12, woman, special needs group)

5. **The system will ensure fairness** (see Extract 5):

   Interviewees also mentioned that e-authentication systems should deal with diversity and ensure equity by supporting everyone with what they need to be successful. Student 11 mentioned that in general, students “*might be hesitant to be monitored and live.” His suggestions were to provide information that participants need to know as well as explaining how e-authentication systems works. In addition, interviewees with special educational needs suggested making the learning experience more pleasurable as well as adapted to individuals' preferences and abilities (e.g. students 13 and 14).*

Extract 5: Students' concerns about their needs and limitations that might impact on e-authentication

Overall my opinion is that it could be an excellent way of e-authentication. However, many people might be hesitant to agree having their typing “monitored” and live due to online security concerns. A way to reassure them might be to **explain in advance** the way this would work (student 11, man, 31- 40 years old)

Learning should be more appealing for people with disabilities, and would in my opinion, enhance student's performance. (student 12, woman, 31- 40 years old)

Having mental health problems, the idea of sitting an examination in a room full of people, makes me extremely anxious. To have this kind of system implemented really would reduce anxiety and make the learning experience more pleasurable (student 13, woman, special needs group)

I find sitting for more than hour an issue and writing with arthritis can also be a problem and are ones I shall also face next year when I sit my first exam. Unless each student is treated on an individual basis, then there could be problems... Will the system ensure fairness? (student 14, woman, special needs group)

Discussion

This study set out to investigate student attitudes to the use of e-authentication in online assessments, with an online student sample that was self-selecting and broadly representative of the OU student body. Here, we discuss briefly the study's findings.

The outcomes in response to the first research question were encouraging although unremarkable, with large majorities of participants correctly identifying what constituted cheating in online assessments. The outcomes in response to the second and third research question, however, were more nuanced and interrelated, and so will be considered together and in more detail. In particular, overall, the findings suggest a broadly positive acceptance of and trust in e-authentication for online assessments by both women and men, with neither group finding the e-authentication tools experienced in this study to be either particularly onerous or stressful. However, the female participants, on average, trusted online assessments more than their male counterparts, and were more confident that e-authentication has the potential to enhance the quality of and trustworthiness of online assessments. On the other hand, while opinions about sharing personal data for e-authentication were more or less evenly split, with around half of the sample being willing to share all the named types of personal data and half being unwilling, male participants were on average more willing to share. This difference points to an issue that successful e-authentication must address: how can e-authentication function if examinees are unwilling to share the types of information on which the e-authentication depends?

Although, as noted, attitudes to e-authentication were broadly positive, there were some differences by age, supporting the earlier findings by Harmon and Lambrinos (2008), Underwood and

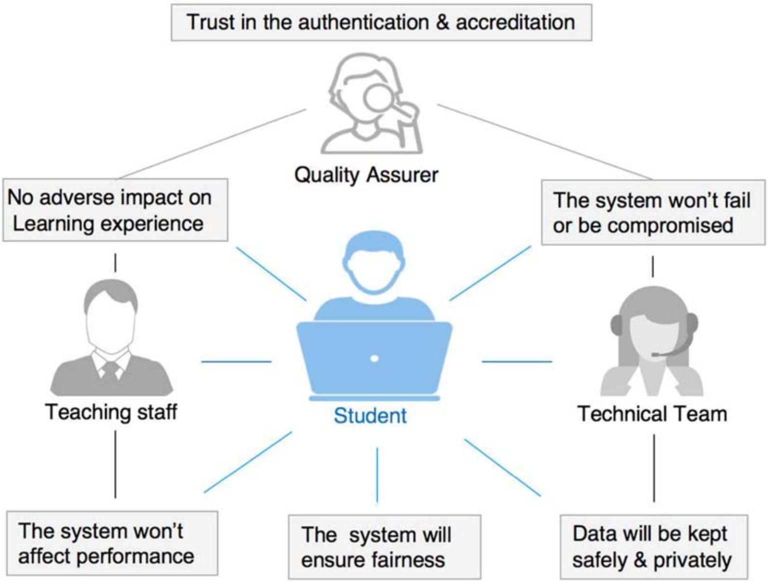
Trust in the authentication & accreditation
Quality Assurer
No adverse impact on Learning experience
The system won't fail or be compromised
Teaching staff
Student
Technical Team
The system won't affect performance
The system will ensure fairness
Data will be kept safely & privately

Figure 4: Model for trust-based adapted e-authentication system

Szabo (2003) and Okada *et al.* (2015). In particular, while older participants, who typically had limited experience of online assessments, were on average more willing to trust the online assessment e-authentication tools, some younger participants were unconvinced that e-authentication had the potential to enhance online assessment. Instead, many of the younger participants saw an institutions' use of e-authentication as an indication that the institution did not trust the students not to cheat. Although a lot of young students share their personal data in their social networks, in the context of e-assessment their attitude is different as they are more concerned about data privacy, security and safety. Finally, despite e-authentication making assessments potentially easier for some disabled students, eg, those with motor disabilities, disabled students had on average various concerns and a relatively negative attitude to e-authentication due to their lack of confidence and concerns on their limitations. Figure 4 presents a model for trust-based adapted e-authentication system with issues to be considered by teaching staff, technical team and quality assurance board.

Final remarks

In conclusion, the outcomes of this study support the use of innovative technologies in assessment, while underscoring the need for the developers of e-authentication systems and pedagogical teams to recognise and respond to the widely differing nature of examinees. Understanding students' attitudes and experiences on e-assessment systems will guide back to the problem.

To reduce plagiarism and cheating in online assessment, a trust-based system for e-authentication which combines various instruments will enable high quality assurance. The perceptions and needs of distinctive users involved in this process through a RRI approach (Von Schomberg, 2011) must be taken into account to increase trust of e-authentication systems (Baneres, Baró, Guerrero-Roldán, & Rodríguez, 2016; Okada *et al.*, 2015).

In this study, students presented various concerns to be addressed by the *TeSLA* project partners in a number of ways: software upgrading, legal safeguards, quality assurance, consent form explaining dealing with some of these concerns; and webinars and newsletters providing useful information for participants. This among other issues will be considered in the next round of pilot studies of the *TeSLA* system.

Acknowledgements

We are grateful to the *TeSLA* consortium, TEA conference reviewers and Prof. Dr. John Richardson for their feedback and support. This work is supported by the European Commission (H2020-ICT-2015/H2020-ICT-2015), Number 688520.

Statements on open data, ethics and conflict of interest

Data can be accessed by contacting the authors.

Ethical approvals were gained from the hosting institution.

No conflict of interest declared.

References

Apampa, K., Wills, G., & Argles, D. (2010). User security issues in summative e-assessment. *International Journal of Digital Society*, *1*, 1–13.

Baneres, D., Baró, X., Guerrero-Roldán, A., & Rodríguez, M. (2016). Adaptive e-assessment system: a general approach. *International Journal of Emerging Technologies in Learning*, *11*, 16–23.

Bermingham, V., Watson, S., & Jones, M. (2010). Plagiarism in UK law schools: is there a postcode lottery? *Assessment and Evaluation in Higher Education*, *35*, 1–14.

Chew, E., Ding, S. L., & Rowell, G. (2015). Changing attitudes in learning and assessment: cast-off 'plagiarism detection' and cast-on self-service assessment for learning. *Innovations in Education and Teaching International*, *52*, 454–463.

EC (2016). *Responsible research and innovation*. Retrieved January 6, 2018, from https://ec.europa.eu/programmes/horizon2020/en/h2020-section/responsible-research-innovation

Edling, R. J. (2000). Information technology in the classroom: experiences and recommendations. *Campus - Wide Information Systems*, *17*, 10–15.

Gao, Q. (2012). Biometric authentication to prevent e-cheating. *International Journal of Instructional Technology and Distance Learning*, *9*, 3–13.

Gras, R., & Kuntz, P. (2008). An overview of the Statistical Implicative Analysis (SIA) development. *Studies in Computational Intelligence*, 127, 11–40.

Hanna, D. E. (1998). Higher education in an era of digital competition: emerging organizational models. *Journal of Asynchronous Learning Networks*, *2*, 66–95.

Harmon, O. R., & Lambrinos, J. (2008). Are online exams an invitation to cheat? *The Journal of Economic Education*, *39*, 116–125.

Harmon, O., Lambrinos, J., & Buffolino, J. (2010). Assessment design and cheating risk in online instruction. *Online Journal of Distance Learning Administration*, *13*, 1–5.

Hastings, N. E., & Dodson, D. F. (2004). Quantifying assurance of knowledge based authentication. In Proceedings of the *3rd European Conference on Information Warfare and Security*. London, UK: ECIW.

IPPHEAE (2013). *Impact of policies for plagiarism in higher education*. Retrieved January 6, 2017, from http://plagiarism.cz/ippheae/

Jelfs, A., & Richardson, J. T. (2013). The use of digital technologies across the adult life span in distance education. *British Journal of Educational Technology*, *44*, 338–351.

Karim, N. A., & Shukur, Z. (2016). Proposed features of an online examination interface design and its optimal values. *Computers in Human Behavior*, *64*, 414–422.

Lerman, I. C. (2016). *Foundations and methods in combinatorial and statistical data analysis and clustering*. London, UK: Springer.

Levy, Y., & Ramin, M. (2007). *A theoretical approach for biometrics authentication of e-exams*. Retrieved January 6, 2017, from http://telem-pub.openu.ac.il/users/chais/2007/morning_1/M1_6.pdf

Okada, A., Mendonca, M., & Scott, P. (2015). Effective web videoconferencing for proctoring online oral exams: a case study at scale in Brazil. *Open Praxis*, *7*, 227–242.

Park, C. (2004). Rebels without a cause: towards an institutional framework for dealing with student plagiarism. *Journal of Further and Higher Education*, *28*, 291–306.

QAA (2016). Plagiarism in Higher Education - Custom essay writing services: an exploration and next steps for the UK higher education sector. Gloucester, UK: Author.

Ullah, A., Xiao, H., Barker, T., & Lilley, M. (2014). Evaluating security and usability of profile based challenge questions authentication in online examinations. *Journal of Internet Services and Applications*, 5, 2.

Underwood, J., & Szabo, A. (2003). Academic offences and e-learning: individual propensities in cheating. *British Journal of Educational Technology*, *34*, 467–477.

Von Schomberg, R. (2011). *Prospects for technology assessment in a framework of responsible research and Innovation* (pp. 39–61). Wiesbaden, Germany: Springer.

Whitelock, D. (2011). Activating assessment for learning: are we on the way with Web 2.0? In M. J. W. Lee & C. McLoughlin (Eds.), *Web 2.0-based-e-learning* (pp. 319–342): Hershey, PA: IGI Global.