Social Sciences & Humanities Open 3 (2021) 100132

Contents lists available at ScienceDirect

Social Sciences & Humanities Open

journal homepage: www.elsevier.com/locate/ssaho

A secure online exams conceptual framework for South African universities

Tembisa Ngqondi [a], Pardon Blessings Maoneke [b,*], Hope Mauwa [b]

[a] Head of School of Computing and Mathematical Sciences, University of Mpumalanga, South Africa
[b] Lecturer in the School of Computing and Mathematical Sciences, University of Mpumalanga, South Africa

ARTICLE INFO

Keywords:
Online exams
Academic fraud
Security
Higher education

ABSTRACT

The massification of higher education has seen South African universities struggle to find a balance between the available resources and quality of education. This has led to university disturbances as witnessed by the recent #FeesMustFall. The use of technology in long distance education offers universities an opportunity to grow and become competitive without putting a lot of pressure on limited resources. This is demonstrated by the use of online learning management systems that have allowed universities to increase enrolments without increasing the number of lecture halls for hosting classes. However, universities find it difficult to host high stake summative assessments online. The postponement and cancellation of exams following the outbreak of coronavirus demonstrate the magnitude of the problem. Electronic exams have always been shunned because of academic fraud. This study uses a literature review to understand academic fraud and respective security measures. The study goes on to propose a framework for online exams grounded in the contextual characteristics of South African universities. The proposed framework can provide universities initial guidelines for online exam adoption.

1. Introduction

The massification of higher education among South African universities has created a challenge on maintaining a balance between the available resources and the quality of education (Hornsby & Osman, 2014; Mohamedbhai, 2014). As such, the 4th Industrial Revolution (4IR) is expected to impact Higher Education Institutions (HEIs) profoundly, as is happening in other sectors (Mwapwele, Marais, Dlamini, & Van Biljon, 2019). It is along these lines that the use of Information and Communication Technologies (ICT) is playing a pivotal role in HEIs as evidenced by the popularity of blended learning and long distance education (Draaijer, Jefferies, & Somers, 2018, pp. 96–108; Lilley, Meere, & Barker, 2016; Ramanathan, Banerjee, & Rao, 2016; Woldeab & Brothen, 2019). While blended learning and long distance education mainly use ICTs to facilitate teaching and learning, it is the use of the electronic medium to facilitate high stake summative assessments that has caught the attention of different stakeholders globally (Draaijer et al., 2018, pp. 96–108; Lilley et al., 2016; Woldeab & Brothen, 2019). The United States (US) introduced the Higher Education Opportunity Act, 2008 that compels HEIs to implement measures that authenticate students whose assessments are facilitated by electronic means to combat the pervasive academic fraud (Bailie & Jortberg, 2009; Barnes & Paris, 2013). The European Union (EU) has since commissioned research projects with the aims of developing secure online assessment tools (Draaijer et al., 2018, pp. 96–108; Okada, Whitelock, Holmes, & Edwards, 2019). Similarly, the academic and private sector are making frantic efforts to develop secure online examination systems (Amigud, Arnedo-Moreno, Daradoumis, & Guerrero-Roldan, 2018).

In South Africa, a policy framework on distance education was proposed in 2017. However, subjects around high stake online assessments appear to have been awakened by the coronavirus pandemic (COVID-19) that necessitated a national lockdown. While some universities are making efforts to implement online learning, there are still questions about how assessments are going to be conducted without compromising the integrity of the qualifications (UNESCO, 2020). Globally, 58 out of the researched 84 countries postponed or rescheduled the dates for conducting examinations (UNESCO, 2020). Most universities have traditional in class, paper-based assessments rather than standardized online assessments (UNESCO, 2020). Accordingly, this study aims to propose a framework for secure online examination system that is suitable for South African universities. Adopting online examination systems can help South African universities enhance their competitiveness and accessibility to students (Draaijer et al., 2018, pp. 96–108). Unfortunately, most of the online examination systems are ad hoc in nature as they focus on one area ignoring other sections (Amigud et al., 2018) something that complicates their adoption in South Africa. Furthermore,

* Corresponding author.
E-mail address: Blessings.Maoneke@ump.ac.za (P.B. Maoneke).

https://doi.org/10.1016/j.ssaho.2021.100132
Received 27 June 2020; Received in revised form 2 November 2020; Accepted 9 February 2021
Available online 8 March 2021

most of the online examination solutions are still at a conceptual level and may never reach production (Amigud et al., 2018). As such, this study uses the literature on online examinations systems and propose a framework that could be considered by South African universities, as a possible remedy. The South African HEIs are complicated by a lack of resources, students from different social and economic backgrounds that calls for special consideration before deciding on intervention strategies for teaching and learning (Davis, 2020). Therefore, the authors herein believe that the proposed framework can be used as a guiding tool by universities that wish to adopt online examination systems. Thus, the concept of online exams is new, hence, this study uses the literature to understand academic threats, controls and use an understanding of the South African context to propose a solution that could be considered for HEIs. The study goes on to propose an online exam implementation process.

The rest of the paper is structured as follows: Section 2 presents an overview of challenges that have interrupted the teaching and learning activities in South African HEIs in the recent past, Section 3 discusses the current status on the use of online assessments globally, Section 4 presents a broad discussion of the factors that motivate academic fraud or dishonesty, Section 5 presents the literature review on online examination models, Section 6 discuss the proposed online examination framework for South African HEIs, Section 7 outlines the online exam implementation process and Section 8 discuss and concludes the study.

2. Interruptions to teaching and learning activities in South African HEIs

Teaching and learning in South Africa's HEIs has had a fair share of disruptions due to students unrest and of recent, due to the global disruption presented by the COVID-19. These developments that impact HEIs motivate the need for online education and examinations. Thus, the reality of using the virtual classroom in HEIs was prompted by various events. In recent years, South African universities have seen a rise in student protests and demonstrations that have erupted for various reasons. In 2015/16, student unrest gained momentum and spread across the country when students protested against fee increase at universities under the #FeesMustFall movement or banner. Some student protests and demonstrations have erupted over frustration with the lack of change in post-apartheid South Africa (Hauser, 2016), such as lack of universities' transformation to address racial inequalities in terms of student and staff composition (Langa, 2017; Hauser, 2016) , especially from historically white universities, lack of a decolonised education system, i.e., lack of curriculum transformation to reflect the lived experiences of African people, including recognition of their scholarly work (Langa, 2017), infrastructural conditions at predominantly black universities and universities of technology (Ndelu, 2017). The effectiveness of the National Student Financial Aid Scheme (NSFAS) has also been questioned and criticised. NSFAS's failure to provide timeous financial relief to indigent students, its slow pace of stipend payments that can be delayed for months and the processes that are used to select the beneficiaries (Ndelu, 2017) have aggrieved students. These protests and demonstrations result in the disruption of universities' core operations, such as lectures or examinations for weeks. Sometimes, these protests and demonstrations result in a complete shutdown of all university operations. When universities eventually reopen, lecturers always have inadequate time to cover all the required course material. To make up for the time lost during the protests and demonstrations, lecturers take difficult decisions to deliver all the course materials meant for the semester; they cover some of the material in passing or give the material to students as reading assignments. In the end, the quality of education offered to the students is compromised, which, eventually, affect the calibre of graduates that universities produce (Bok, 2017).

In addition to student unrest, the need to find an alternative method of teaching and learning at HEIs has been necessitated by the COVID-19 pandemic, which has affected the delivery of face-to-face teaching and learning. The South African Minister of Higher Education, Science and Technology reports that about 2.5 million students and staff were locked out of HEIs due to the COVID-19 pandemic (Nzimande, 2020). On the March 24, 2020, the same Minister (Nzimande, 2020) reported of presentations that were made by relevant stakeholders on their electronic learning (e-learning) emergency strategies as measures for promoting the continuity of teaching and learning following the outbreak of COVID-19. These events compliment the already existing efforts to promote online education eventhough progress thus far is less satisfactory (Webbstock & Fisher, 2016). South Africa's University of Pretoria first introduced a learning management system that facilitates online education in 1998 (Bagarukayo & Kalema, 2015). More than two-decades later, South African HEIs are still struggling to fully utilize online education (Bagarukayo & Kalema, 2015; Mpungose & Khoza, 2020; Webbstock & Fisher, 2016) ; . An effective use of online education should involve the use of various graphics that are pedagogically coherent and address different learning styles of students (Ferran, González, Esteves, Gómez Reynoso, & Guzman, 2019; McLoughlin & Luca, 2002). Hence, online education goes beyond simple acts of posting videos or PowerPoint slides on learning management systems. While the conducting of online education is key for the success of online examinations, it is important to highlight that online education is beyond the scope of this study. This study focuses on exploring the implementation of online examinations. The authors of this study argue that the ongoing efforts that promote the use of online education in South Africa are paving the way for online examinations. Hence, it is worth exploring the characteristics of an online examination system suitable for South African HEIs.

3. The use of online assessments

Examinations have been in use to assess one's competence since "the Han Dynasty in 207 BCE" (Apampa, Wills, & Argles, 2010; Kuyoro, Maminor, Kanu, & Akande, 2016). It should be noted that the introduction of the blended learning model has seen many universities adopting online learning management systems (LMS) that facilitate online formative assessments such as assignment or project submission and quizzes. Little progress has been made in adopting online exam management systems for summative assessments that mainly contribute towards a student's final mark (Apampa et al., 2010; Draaijer et al., 2018, pp. 96–108; UNESCO, 2020). There are fears of academic dishonest and identity misrepresentation (academic fraud) in online exams something that could jeopardize the institutional integrity and the credibility of qualifications on offer (Barnes & Paris, 2013; McGee, 2013; Paullet, Douglas, & Chawdhry, 2014). Though debatable, academic fraud is more pronounced in online exams when compared to traditional exams that are written under the supervision of a proctor because, online environments allow students to work independently with little or no form of supervision and monitoring (Barnes & Paris, 2013; King, Guyette, & Piotrowski, 2009; McGee, 2013).

The prevalence of academic fraud cast a dark cloud over distance education something that forced the US to promulgate a Higher Education Opportunity Act in 2008 (Barnes & Paris, 2013; McGee, 2013). The Policy Statements on Distance Education mandate academic institutions offering online learning services to ensure "the integrity of student work and the credibility of degrees and credits" (SACS: CS 3.4.6 and CS 3.4.10 2008 in McGee, 2013). Hence, universities are required to implement measures for promoting academic honesty otherwise they risk revocation of their accreditation. The growth and potential future of online examination systems in the US has attracted the private sector that is also offering online exam services to HEIs. For example, the US's Western Governors University has been using third parties to facilitate more than 36 000 online assessments (Draaijer et al., 2018, pp. 96–108).

The concept of online examination systems remains new in the EU (Draaijer et al., 2018, pp. 96–108). Belgian universities are among the early adopters of online examination systems in the EU. The EU recognizes the use of an online examination system as a strategic opportunity for HEIs

to go global. Hence, the EU has since commissioned projects on online examination systems, for instance, the "Online Proctoring for Remote Examination" (OP4RE) and the Trust-based e-Assessment System for Learning (TeSLA) (Okada, Whitelock, Holmes, & Edwards, 2018, pp. 109–122; Okada et al., 2019). Elsewhere, for example in Australia, there are suggestions that universities can explore alternative ways of assessing students instead of using online exams because of a lack of ICT supporting infrastructures (Cramp, Medlin, Lake, & Sharp, 2019). In South Africa, the Department of Higher Education and Training (2017) proposed a policy framework for distance education and the hosting of online assessments. The policy states that universities offering distance education must make an effort of putting in place *"an assessment and examination regime that ensures integrity and credibility"* (Department of Higher Education and Training, 2017, p. 19). Both the South African and US policy on online assessments have been castigated for their failure to provide a prescriptive guideline on what constitutes an identity authentication system (Amigud et al., 2018; Apampa et al., 2010; Barnes & Paris, 2013; McGee, 2013; Paullet et al., 2014). Mechanisms for user authentication are vast and offer different degrees of accuracy (Amigud et al., 2018; Apampa et al., 2010; Barnes & Paris, 2013; McGee, 2013; Paullet et al., 2014).

3.1. The impact of online examination security systems on students

The growth in popularity of blended learning and distance education gave birth to online exams (Ramanathan et al., 2016). This has seen several scholars gaining a keen interest to understand the effects of online exams on students considering that, online exams are conducted in an environment that differs from that of the traditional in-class paper-based exams (Cramp et al., 2019). For example, Beust et al.'s (2018) longitudinal study sought to compare traditional exams against an online exam that was monitored in real-time by a remote proctor using a webcam. Their online exam was arguably set up in a manner reported in Lilley et al. (2016). Beust, Duchatelle, and Cauchard (2018) found that students' performance in traditional and online exams were comparable. However, delays were observed in online exams where the students were asked to draw a diagram. Also, 2% of the students had privacy concerns, a single incident of cheating was noted and not more than 5% experienced technical problems. Approximately 70% indicated that remote monitoring made it difficult to cheat and 80% indicated that they would write an online exam again if given a chance (Beust et al., 2018). Similarly, Lilley et al. (2016) note that remote live proctor made most students feel supported and worry less something that allowed them to concentrate on their exam. Also, some students felt that this enhanced the credibility of their course and felt "valued by the institution" (Lilley et al., 2016, p. 3). However, a group of students were anxious because of a long authentication process while United Kingdom-based students expressed concern over giving a stranger access to their desktop and personal information.

Similarly, Weiner and Hurtz (2017) concluded that the performance of students in online remote proctored exams was comparable to that of students who wrote their exams in "traditional test centre proctoring" (p. 18). However, if these exams are written asynchronously, students who write online exams often get higher marks mainly because of cheating (Feinman, 2018). Nonetheless, students generally find online proctored exam conditions favourable (Weiner & Hurtz, 2017). These views were shared by participants in Okada et al. (2018, pp. 109–122). Thus, the students expressed a positive attitude towards online exams and also felt that this exam mode was not stressful.

However, other studies report contrasting findings in particular to the impact of online exams on students. Cramp et al. (2019) note that online exams leave students feeling anxious, posing a cognitive burden on them even though this may not always result in poor performance when compared to paper-based exams. On the contrary, study findings by Woldeab and Brothen (2019) on undergraduate students at a US university points to the fact that performance in online proctored exams is extremely low. This poor performance is a result of using online proctors, a move that is believed to be upsetting, and high anxiety among students caused by online exams (Woldeab & Brothen, 2019). Similarly, James (2016) observes that 30% of the students (first-year students) who took an online exam "had a very ordinary or bad experience" (p. 10). This was corroborated by high drop-out rates as students abandoned online exams for traditional exams. James (2016) went on to conclude that first-year students who often have less experience in online education are more likely to face technical difficulties in online exams. Another study by Okada et al. (2018, pp. 109–122) confirms that older students with experience in online exams are more willing to trust online exams when compared to younger students who prefer traditional paper-based exams. There are suggestions that technical challenges faced by students during an online exam are some of the causes of high anxiety. For example, James (2016) notes that failure to authenticate one's identity or requiring multiple attempts to do so increases anxiety. As such, providing real-time support for students writing online exams can play a key role in instilling satisfaction, confidence and reducing anxiety.

4. The nature and reasons for academic fraud

To find a solution for academic fraud during online exams, it is worthwhile addressing at least the following two questions:

- What are the factors motivating academic fraud during online exams?
- What are the fraudulent activities likely to be done by students during online exams?

Ballentine et al. (2019); Bailie et al. (2009) and King et al. (2009) suggests that the fraud triangle can be used to explain factors that motivate academic fraud or dishonesty. The fraud triangle or theory proposed by Donald Cressey in 1950 is widely used in the corporate world to explain why people commit fraud (Kassem &Higson, 2012). Furthermore, the fraud triangle can help one identify the fraudulent activities that could be done by students and how these fraudulent activities are likely to occur if there are no adequate controls. The fraud triangle proposes that pressure/incentive, opportunity and rationalization/attitude are three conditions that should be met if one is to indulge in fraudulent activity. In addition, Peled, Eshet, Barczyk, and Grinautski (2018) observes that personality traits can help predict one's likelihood to commit academic fraud. Together, these conditions or factors are explained next regarding online examinations.

4.1. Pressure/incentive

The need to commit academic fraud arises when the prevailing circumstances are forcing one into assuming an option that violates their position of trust. Pressure/incentive can be seen as the motive behind a fraudulent activity (Kassem & Higson, 2012). This motive to commit academic fraud may result from internal or external pressures (McGee, 2013). For example, internal pressure emanates from a desire to attain better results, pass a course or the fear of failing and procrastination or laziness (Ballentine et al., 2019; King et al., 2009; McGee, 2013; Paullet et al., 2014). However, students who find a course interesting or useful to them are less likely to cheat but cultivate a need to understand the course and test themselves (Ballentine et al., 2019). External pressures may include pressure from parents or guardians or teacher towards a student that he/she performs well (Ballentine et al., 2019; McGee, 2013). Also, fear of losing money or a desire to win a reward (Ballentine et al., 2019) or fear of losing study grants could also potentially drive students towards academic fraud. Exactly 20% of the students at South African universities are funded by the NSFAS (Bhorat, Kimani, & Pillay, 2018). Students who pass their exams under the NSFAS funding scheme benefit from part of their loan being translated into a bursary something that reduces the total amount to be repaid (Bhorat & Pillay, 2017). Underperforming students risk losing their study grants. Hence, these factors are likely to put South African university students under immense external pressure to commit academic fraud.

4.2. Opportunity

The perceived opportunity is when a fraudster identifies a way to take advantage of his/her "position of trust" and commit fraud without being caught. Thus, it is the existence of an opportunity that makes one commit fraud provided the risk of getting caught is low (Ballentine et al., 2019). Otherwise, the existence of pressure or motive alone is not enough to motivate one into committing fraud. Paullet et al. (2014) suggest that students are more likely to indulge in online exam fraudulent activities because they are under the pressure of vast opportunities to do so. Nearly a quarter of 824 students cheated in electronic exams and 42% indicated that they would cheat again if the opportunity arises (Chapman et al., 2004 in Peled et al., 2018).

Online academic fraud opportunities can be technology or non-technological based. In technology-based opportunities, students can manipulate the technology in a way that would assist them to commit academic fraud. For example, students can take advantage of weak identity controls and find someone to write their exams or collude with others and share information by email, mobile phone or skype (Amigud et al., 2018; Okada, Whitelock, Holmes, 2019; Paullet et al., 2014; Ullah, Barker, & Xiao, 2017) or cause technological disruptions with the aims of making excuses over the exams (McGee, 2013; Paullet et al., 2014). These include internet connectivity disruptions or instigate computer malfunctioning with the hope of getting an opportunity to re-write the exam (McGee, 2013; Paullet et al., 2014). However, these malfunctions could be genuinely resulting from a poor internet connection, using outdated hardware and operating systems (Davis, Rand, & Seay, 2016). Some students may try to access the exam or download the exam before the scheduled exam date (McGee, 2013). Furthermore, students could use other technological devices or simply open additional webpages and search for answers (Paullet et al., 2014). Even when webcams are used for monitoring, students have been found colluding with others by using glasses equipped with wireless cameras for transmitting questions and answers (Feinman, 2018) in some cases the legitimate student faces the webcams while someone else is typing on the keyboard (Nader, DeMara, Tatulian, & Chen, 2019).

Non-technology based opportunities that could be exploited by students include using notes or textbooks or asking friends for answers during an online exam (Paullet et al., 2014). In addition, a lack of clear instructions, "little chance of being caught", and even caught, there might be no punitive measures (McGee, 2013, p. 5) are some of the non-technology based opportunities that could be exploited by students during an online, remote exam. Using online proctors and constant monitoring and evaluating online security measures can help mitigate technical and non-technical based opportunities (Ballentine et al., 2019).

4.3. Rationalization/attitude

Rationalization/attitude is some form of justification used by fraudsters when committing fraud thereby making the act acceptable in their eyes (Kassem & Higson, 2012). For instance, 73.6% of the students that took part in a study by King et al. (2009) are of the view that it is easy to cheat in an online exam than in traditional exams. Similarly, McGee (2013) states that online exam fraud may occur because students feel that "everyone else is doing it" (p. 5). Lastly, students assert that it is not their responsibility to prevent or avoid academic fraud (Carpenter, 2006 in Ballentine et al., 2019). Instead, they believe it is the instructor or the institution's responsibility. This suggests that students may engage in academic fraud unknowingly (Paullet et al., 2014) because they believe it is not their duty to make available information on what is expected of them in online exams (McGee, 2013). This view is cemented by a significant decrease in online exam and quiz cheating following a university's proclamation of "honor codes or academic integrity policies" (LoSchiavo & Shatz, 2011 in Paullet et al., 2014, p. 371). In addition, the dominance of cheating among undergraduate students when compared to students who are at an advanced level in their studies further cements the thought that the lack of knowledge and inexperience in online exams among first-year students (James, 2016; Okada et al., 2019; Woldeab & Brothen, 2019) promotes cheating. As a result, understanding the attitude of students can help mitigate the occurrence of academic fraud.

4.4. Personality traits

Peled et al. (2018) evaluate the influence of personal traits; conscientiousness, emotional stability, agreeableness, extraversion and openness to experience; in academic fraud. Individuals with conscientiousness personality traits are those who like planning hence, they are organized or follow rules and norms, and are driven by achieving set goals. On the other hand, individuals who portray emotional stability have a good sense of security and cannot always be pressured into actions they do not agree with. In addition, agreeable individuals "are likeable, warm, trusting, and concerned with the welfare of others" (Peled et al., 2018, p. 3). Extraversion individuals enjoy social situations and are usually positive, full of energy and outgoing in nature. Lastly, openness to experience individuals is said to be curious and open to new experiences. These traits may influence the intent to commit academic fraud positively or negatively (Peled et al., 2018). For example, students with an extraversion personality are more likely to cheat in an online exam. However, university students who study in an environment where academic fraud is strongly discouraged and have personality traits that include "conscientiousness, emotional stability, agreeableness, and openness to experience" are less likely to cheat in online exams (Peled et al., 2018). Hence, understanding the personality traits of the students can help shape the implementation of an online learning system.

5. Literature review on online examination security models

This section discusses different online examination security models. Authentication can be based on *what one is - biometrics*, *what one has - tokens or identity documents* and, *what one knows – passwords or question and answer the challenge*. Due to the magnitude of risks in online exams (Vegendla & Sindre, 2019), there is wide use of effective and multi-factor authentication mechanisms (Beust et al., 2018; Lilley et al., 2016; Okada et al., 2019). These include biometrics based authentications, live remote proctor, question and answer challenge, and keystroke dynamics. In addition to these technological security configurations, the authors acknowledge the need for supporting frameworks such as policies and a clear outline of how online exams should be set (Bailie & Jortberg, 2009; Ballentine et al., 2019; McGee, 2013). The next sections discuss the authentication mechanisms used in online exams.

5.1. Biometrics solutions

The biometric driven security solutions reported in the literature are either based on multi-biometrics or multi-factor authentication with biometrics playing a central role. Some of the security solutions presented here are meant to operate as a virtual proctor but some require the presence of a live-remote human proctor for exam monitoring (Apampa et al., 2010; Sabbah, 2017; Traoré et al., 2017, pp. 73–81; Urosevic, 2019).

5.1.1. *Apampa, Wills and Argles' (2010) multimodal biometric solution*

Urosevic (2019) and Apampa et al. (2010) suggests that an online examination security must be grounded in biometric-based authentication mechanisms. For instance, Apampa et al. (2010) propose a security model with three modules namely the authentication, tracking and classifier module. The authentication module is activated first where students are authenticated by use of multimodal biometrics: face and fingerprint. Once authenticated, the students are moved into the tracking module. The tracking module captures a video and location details of the student writing the exam for continuous authentication. The video recording focuses on face recognition and monitors head movement

during the exam. It is a must to have facial and voice recognition constantly monitoring students during an exam (Urosevic, 2019). Furthermore, the classifier module receives video recording from the tracking module and constantly rate the risk levels depending on the facial and head movements of the student. Low risk means that the student can continue with the exam but the elevated risk would see the student classified as a fraud suspect. High-risk level will see the student being interrupted and forced to re-authenticate, a task that is done by the authentication module.

In addition, Paullet et al. (2014) suggest an online examination security model that is almost similar to that of Apampa et al. (2010). Paullet et al. (2014) recommend the use of biometrics for authentication, webcams for monitoring students during the exam and carefully analyzing students' work for similarity or plagiarism. Furthermore, Paullet et al. (2014) recommend tracking keystrokes, controlling applications that can be opened by students during the exam and conducting background sound checks. Together, these measures are expected to address several security vulnerabilities in online exams such as impersonation, collusion, searching for answers on the internet and so on. In particular, continued authentication assumes the role of a proctor to constantly monitor and supervise students as done in traditional exams.

5.1.2. Traoré et al.'s (2017) multimodal biometric solution

Traoré et al. (2017) propose an online exam system based on continuous multimodal biometric authentication. They argued that most online exam systems authenticate students during login but do not go on to verify if the legitimate student is the one writing the exam. Their authentication system is based on face recognition, mouse and keystroke dynamics. Participants were invited to enrol by taking a 3-min long facial video that was used to generate the facial signature (Traoré et al., 2017, pp. 73–81). Once the student is logged in, the exam system recorded the whole exam session using a webcam. An alarm would be raised if the student leaves the chair or engage another person to write the exam or if many students are detected within the exam environment. Though successful, the system was affected by technical glitches such as a drop in the network connection or leaking memory. Furthermore, poor lighting affected authentication effectiveness. These technical glitches may still present opportunities for students to commit academic fraud as discussed under the fraud theory.

5.1.3. Sabbah's (2017) bimodal biometric solution (SABBAH)

Sabbah (2017) proposes a Smart Approach for Bimodal Biometrics Authentication in Home-exams (SABBAH) that offer continuous authentication in online exams. Sabbah (2017) states that an online exam security system should seek to address tenants of security namely confidentiality, integrity, availability and authenticity. SABBAH makes use of a multimodal authentication mechanism that is composed of biometrics (facial recognition, fingerprints) and keystrokes dynamics. Typing patterns are used for keystrokes dynamics together with a fingerprint scanner embedded in a mouse. In addition, a webcam is used to monitor students during the exam. Fingerprints are used during the initial authentication and monitoring the presence of a legitimate student if the webcam stream is down. Similarly, keystroke dynamics are used to continuously authenticate the identity of the examinee. Data from the webcam, fingerprints and keystroke dynamics is fed into an algorithm, collectively analyzed in real-time and give output on exam fraud risk ratings. Hence, Sabbah's (2017) system is meant to operate as a remote independent proctor. For SABBAH to work, students have to be enrolled first where a fingerprint, keystroke dynamics and a short video are captured to form a student's signature. This signature will be used during the initial authentication and continued monitoring (Sabbah, 2017).

In addition, SABBAH has the capabilities of detecting technical faults that include deactivating the keyboard or mouse or webcam. Similarly, switching off the computer, internet disconnection and system errors could be detected. Sabbah (2017) suggests that such errors can be evaluated to see if they have been initiated by students, of which, that would constitute to exam cheating, otherwise "no penalty will be applied". Other violations such as impersonation, producing noise, sharing information and other forms of suspicious movements can be detected, weighted and a warning is given. The examination could be terminated if the magnitude of violations are considered to be too high. Tests and evaluations show that SABBAH has a success rate of 96.3%. SABBAH managed to combat impersonation, ensured confidentiality, integrity and system availability. This success rate implies a failure rate of 3.7%, a rate that may be too high for international standards. The European standard for access-control systems (EN-50133-1) recommends a miss rate of no more than 0.001% (**CENELEC. European Standard EN 50133–1 in** Killourhy & Maxion, 2009). In addition, SABBAH has a relatively low fault tolerance rate of 73.9%.

5.1.4. Adaptive TeSLA

The European Union-funded project: TeSLA, motivated the use of face recognition, anti-plagiarism software, keystroke dynamics and, a question and answer the challenge in user authentication (Okada et al., 2018, 2019, pp. 109–122). Ullah·Hannan and Barker (2019) and Urosevic (2019) makes a similar recommendation of a question and answer the challenge that uses data gathered from a student's profile. The question and answer challenge can also be used at specific checkpoints during the exam to confirm the identity of the student writing the exam in addition to initially authenticating students (Urosevic, 2019). Urosevic (2019) is of the view that such a technique has to be implemented in a multi-factor authentication system in order to be effective. Accordingly, Okada et al. (2019) use keystroke dynamics to monitor the typing behaviours of the examinee. Furthermore, face recognition and background sound checks are additional security measures used in TeSLA together with anti-plagiarism software for detecting similarities across examinees' answers (Okada et al., 2018, pp. 109–122). However, nearly half of the participants were unwilling to share their data for use in a question and answer challenge probably for privacy, security and safety reasons (Okada et al., 2019). This is more pronounced among females (Okada et al., 2018, pp. 109–122). Refusal to avail such personal data threatens the viability of the dynamic question and answer challenge in student authentication.

5.2. Live remote proctor

Live remote proctor involves a proctor monitoring a student remotely by use of a webcam. In addition, this set up can also make use of a virtual remote proctor that uses an algorithm to predict actions that accumulate to online exam cheating. We also admit that this technique can be seen as biometric-based given the wide use of visual images in continuous authentication and monitoring.

5.2.1. Lilley et al.,'s (2016) academic remote-live invigilation

Lilley et al. (2016) evaluate a biometric-based remote proctoring online exam system. Their solution was pilot studied using students from Egypt, Kenya, Saudi Arabia, Slovakia, Trinidad and Tobago, United Kingdom and Zambia. Students are required to register for the exam in advance. Registration will see student details, date and time for taking the exam captured. Once registration is done, a remote proctor is notified of this incident so that he/she is available when the exam starts. Students will then login into their profiles on the exam date and time. A username and password are used for initial login. After logging in, students will be required to download and install software that activates their webcam and provide remote desktop access to an online, remote proctor. The following set of authentication activities will be done once the proctor and the student are connected:

1. The student is asked to present some form of identification e.g. a passport through the webcam. The proctor inspects details presented in the identification document against those provided during registration. In addition, the student's image in the identification card will

be compared to that of the person sitting for the exam and the one that was captured in the system if any. No data will be captured during this step for privacy reasons.
2. The proctor captures "digital photo of the student and stores this on the service provider system for future reference."
3. "US citizens are required to answer a series of multiple-choice challenge questions based on public records; a typical example would be selecting a previous postcode from a choice of four. Non-US citizens are typically required to present a second form of photo identification.
4. Following authentication, students are asked to pan over their work area using their webcam and hold a reflective surface to the camera to ensure there are no disallowed materials or persons present" (Lilley et al., 2016, p. 2).

Once authenticated, the proctor reads exams rules to the student. The student can then proceed to login into the exam platform. In some instances, it is the remote online proctor who has the credentials to grant student access to the exam. The proctor will monitor the student for any unusual behaviour using the webcam, background sound checks and observes the desktop of the student remotely. Beust et al. (2018) suggest that a mirror could be included in this setup, probably at the back of the student such that the examinee's screen and keyboard are reflected the remote proctor to see via the webcam. Students will be warned if they are judged to have behaved in unusual behaviour. If this persists, the proctor is expected to gather evidence that will be used against the student. This academic live invigilation is arguably the system that is used by the EC-Council, an institute that offers online computer security exams, to facilitate its remote proctored online exams.

5.2.2. *Davis, Rand and Seay's (2016) remote proctoring*

Davis et al. (2016) report of the Remote Proctor Now (RPN), a solution provided to US universities by a third party. Students access the online exam through a learning management system and download the application that enables them to access RPN. Once on RPN, audio, video and bandwidth are evaluated to establish if these meet the minimum requirements for the online exam. This is followed by steps 1, 2 and 4 in Lilley et al. (2016). The exam session is recorded and a webcam is used by a remote proctor to monitor students in real-time. The platform used by Davis et al. (2016) has practice questions that allow students to familiarize with the exam environment before the actual exam.

5.2.3. *Chuang, Craig and Femiani's (2017) time delay and heard pose authentication system*

Chuang, Craig, and Femiani (2017) propose an automated online exam cheating detection system based on the students' behaviour. Their system uses an algorithm that predicts cheating when fed with data on Visual Focus of Attention (VFOA) and time delays in responding to exam questions. Data collection and analysis went on to prove that one's head movement relative to the monitor (VFOA) and delayed response to exam question(s) could successfully (76% accuracy) predict cheating behaviours (Chuang et al., 2017). For instance, the delayed response may be instigated by a student's acts to explore alternative sources of answers that may involve collusion. Nonetheless, data on VFOA and delaying time is gathered in real-time as students are writing the exam. This enables the exam authentication system to continuously authenticate and detect any form of cheating that can be done by a student in real-time during the exam. This system is designed to operate as an independent remote real-time virtual proctor without human intervention. However, a finding that one out of 10 incidents were erroneously flagged as cheating suggests that the system is yet to attain acceptable false-positive rates. This false-positive rate is too high considering that the European standard for access-control systems recommends a false positive of less than 1% (Killourhy & Maxion, 2009). Such false-positive incidence during user authentication or when detecting fraudulent incidences may spark unnecessary anxiety thereby affecting the performance of students in online exams (James, 2016; Woldeab & Brothen, 2019).

5.3. *Question and answer challenge*

This technique involves students being asked a set of questions they should answer to prove their identity. These questions can be pre-set or dynamically set using background data. However, this technique is hardly used independently as already noted in the case of TeSLA discussed earlier.

5.3.1. *Ullah·Hannan and Barker's (2019) dynamic profile question*

Ullah·Hannan and Barker (2019) used a question and answer the challenge to mitigate impersonation. This technique requires that students register their answers before the authentication session of question and answer (Ullah·Hannan & Barker, 2019). However, there are concerns that students can always share questions and answers with their impersonators. As such, Ullah·Hannan and Barker (2019) designed a question and answer the challenge in which questions for authenticating students were developed in the background using profile data that was generated as students went about their learning activities. Hence, it is referred to as dynamic profile questions. Ullah·Hannan and Barker's (2019) system effectively authenticated students with an accuracy rate of 99.5%. However, the dynamic profile questions could still be breached by impersonators who shared answers using mobile phones. Ullah·Hannan and Barker (2019) go on to suggest that the time delay in responding to questions could be used to effectively distinguish an impersonator from a genuine student. Nonetheless, using time delay to detect and justify acts of academic fraud with no additional supporting evidence may be difficult. Ullah et al. (2017) recommend a remote proctor based on a live video monitoring together with a secure web browser for this technique to be effective.

6. The proposed online examination framework for South African HEIs

The available online examination frameworks are either at a conceptual stage or are techno-centric (Amigud et al., 2018) with the assumption that other stakeholders such as students, examiners and administrators would automatically fit in. Such solutions may not be feasible in South Africa given differences in social standing among the students and unequal distribution of ICT infrastructure. In addition, the power of the students in influencing the operations of South African HEI was demonstrated during the #FeesMustFall unrests. Any solution that is imposed on students without a careful consideration risk rejection. As such, this study proposes a holistic online examination framework for South African universities. This study assumes the Socio-Technical Theory and develops a framework of online examinations for South African universities. The Socio-Technical Theory advances the thought that an information systems problem can be addressed by focusing on both the social and technical sub-systems. This is so because the success of an information system or technical solution depends upon its social rather than technical implications (Author, 2020). Accordingly, this study's proposed online examination framework is composed of two modules: the authentication and continuous monitoring (technical sub-systems), and online examination system enablers (social sub-systems).

6.1. *Authentication and continuous monitoring module*

This component enrols, authenticate and goes on to continuously monitor the student writing the exam for support and real-time inspection of fraudulent activities (Amigud, Arnedo-Moreno, Daradoumis, & Guerrero-Roldan, 2016). We argue that continuous monitoring should not only be meant to monitor for fraudulent activities as done in the literature but to offer students support and the necessary guidance in a manner that help suppress anxiety. The activities of this module can be split into three phases namely student enrollment and standardization, authentication and continuous monitoring and termination. These phases are explained next.

6.1.1. Student enrolment and standardization

The literature suggests that most authentication mechanisms require one to enrol factors or traits to be used in the authentication. These will become a student's signature when accessing the online exam. Apampa and Argles (2010) analyzed different electronic assessment (e-assessment) security solutions and concluded that any solution that does not involve the use of biometrics is inadequate to address online exam threats. This study recommends the use of multimodal biometrics for user authentication. Fingerprints and face recognition will be used to authenticate students. As such, students who intend to write an exam are required to register and submit their fingerprints and a 3-min long facial video clip that will be used to generate a student's digital signature. Laptops with a fingerprint scanner can be used to scan students' fingerprints. A webcam can also be used for capturing a video for generating a student's facial signature. The HEI should have guidelines on the required amount of lighting and angles at which the video clip should be taken. Wearing of glasses and hats should be discouraged during the generation of a facial signature. In addition, HEI should recommend minimal specifications for a webcam to ensure consistent visual images for the system. Having standardized computer hardware, video cameras and software help maintain a consistent system performance across the board (Davis et al., 2016; Weiner & Hurtz, 2017).

In addition, HEIs should have a guideline on the minimum recommended internet speed that is required for one to write an online examination. Therefore, tests will need to be done during this phase to establish if the internet speed in the student's environment meets the minimal recommended speed. The distribution of broadband is not even in South Africa, hence, it is important that, during enrollment, a student's internet speed is evaluated. Students with a poor internet speed will be required to find a location with the recommended minimal internet speed for the exam. Only those with the minimum recommended internet speed should be allowed to enroll for an online exam. Furthermore, the student's geographical location data should be automatically determined and captured (Apampa et al., 2010; Okada et al., 2019). This data can be useful when investigating academic fraud cases or for other administrative issues in case students have complained related to their environmental location. Provisions for updating the internet speed and geographical location should be availed to students should there be a need for changes. Data gathered during this phase should be transferred using a secure channel and should be stored in an encrypted format. The exam registration form should be attached with terms and conditions indicating the university's adherence to local and international data privacy laws (Amigud et al., 2018; Lilley et al., 2016; Okada et al., 2019). Lastly, this phase can also be used to communicate the university's stance on academic fraud. Fig. 1 summaries activities of exam registration.

6.1.2. Student authentication

The literature review identified different authentication mechanisms. The proposed initial authentication for South African universities online examination system aligns to propositions in Davis et al. (2016) and Lilley et al. (2016). Davis et al. (2016) and Lilley et al.'s (2016) proposed authentication measures have received wide use in the industry. Accordingly, the students will log in using a username and password. This is followed by video, audio and bandwidth tests. The student goes on to download, install and open software that gives remote proctor access to the student's desktop, activates the webcam and audio. At this point, a student can present a form of identification and display it to the remote proctor via a webcam. The remote proctor should confirm details in the presented identification card against those of the person who registered for the exam. Next, the student should further confirm identity by use of fingerprint and facial recognition system. Once identity has been confirmed, the remote proctor should ask the examinee to pan over their work area as explained in Lilley et al. (2016). Combining a remote proctor, fingerprints and facial recognition provides a solid authentication that can overcome impersonation and bringing forbidden material into the exam environment (Amiguda et al., 2016; McGee, 2013; Paullet et al., 2014; Vegendla & Sindre, 2019). Passwords can easily be shared and keystroke dynamics have a higher rate of false positives (type I errors) and false negatives (type II errors), hence, they may not be suitable for online exam authentication. In addition, virtual online exam systems that operate independently without human intervention as reported in Chuang et al. (2017) may not be viable due to high false positives and a lack of basic ICT skills among South African students. Approximately 56% of South African university students lack basic ICT skills to operate a computer (Oyedemi & Mogano, 2018). Support from a remote proctor is expected to reduce anxiety among the students so that they focus on their exams (Cramp et al., 2019; Lilley et al., 2016). Once authenticated, students may now proceed and write the exam under the continuous monitoring and termination phase. These activities are summarized in Fig. 2. Section 6.2.2 explains processes that should be followed during the conduct of the exam (Fig. 3).

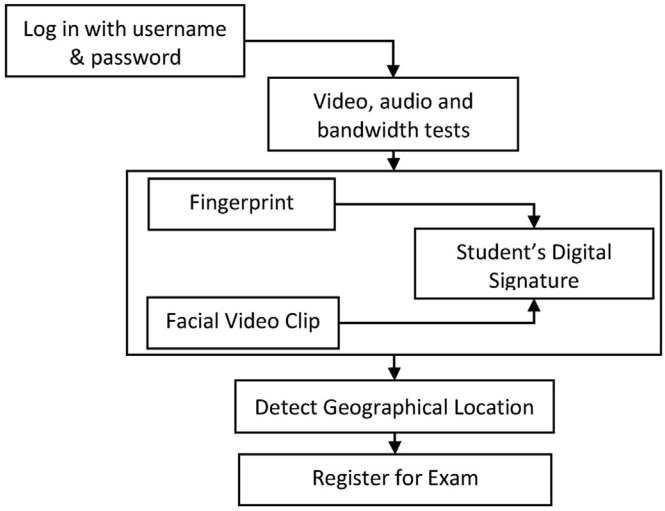

Fig. 1. Exam registration.

6.1.3. Continuous monitoring and termination

Continuous monitoring can be done by use of a remote live proctor, keystroke dynamics, question and challenge, biometrics or a combination of these (Apampa et al., 2010; Lilley et al., 2016; Sabbah, 2017; Traoré et al., 2017, pp. 73–81; Urosevic, 2019). Authors in this study recommend the use of real-time automated background sound checks, facial recognition, time delay and head pose for continued monitoring. In addition, the exam platform should use a lockdown browser such as Respondus that controls applications that can be opened by students during the exam (McGee, 2013; Paulet et al., 2014). Overall, the idea is to reduce the reliance on full-time remote proctors and cut costs. Given that a lot of students are likely to write the same exam at the same time, keeping full-time remote proctors for the duration of the exam may be costly. However, visual recordings by a webcam during the entire exam can be used for facial recognition. Besides, these recordings can be used to monitor time delays when responding to questions and head movement as done by Sabbah (2017) and Chuang et al. (2017). Together, data from background sound checks and the webcam should be fed into an algorithm that can predict the occurrence of exam cheating in real-time. These measures have been found minimizing chances of examination fraud through the use of forbidden material, impersonation, assistance/collaboration, distance communication and whispering (Vegendla & Sindre, 2019). The risk of exam cheating can be ranked as done in Sabbah (2017) and Chuang et al. (2017) in such a way that an alarm can be sent to the remote proctor for immediate intervention should the risk be deemed moderate or high. At this point, the remote proctor can warn the student or initiate the termination of the exam, making sure that enough evidence has been gathered. Similarly, technical faults have to be

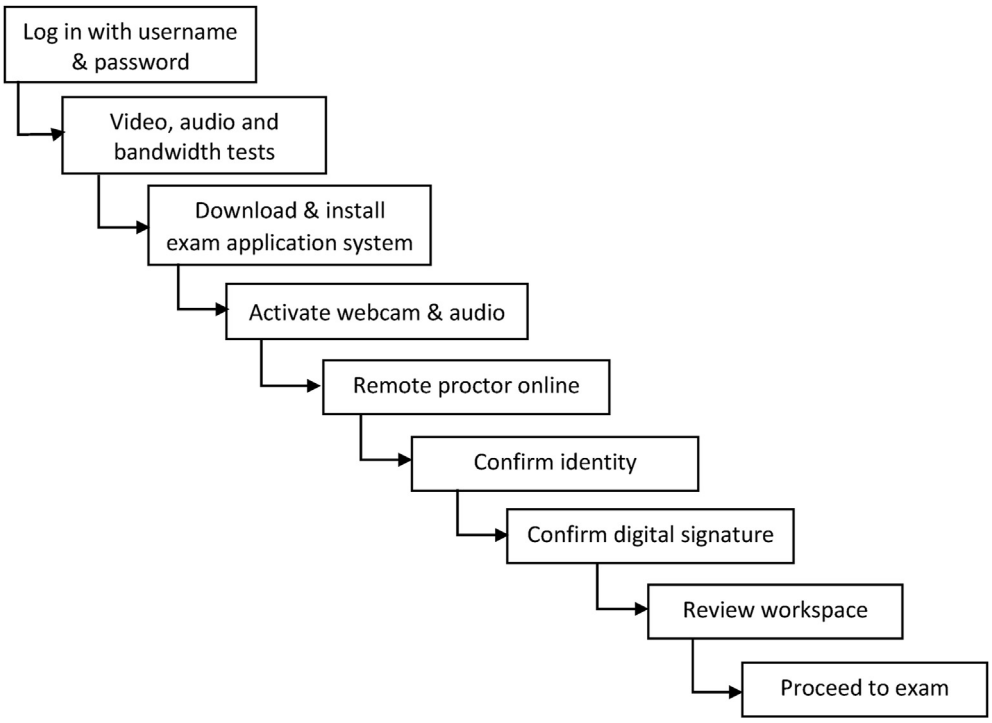

Fig. 2. Exam authentication steps.

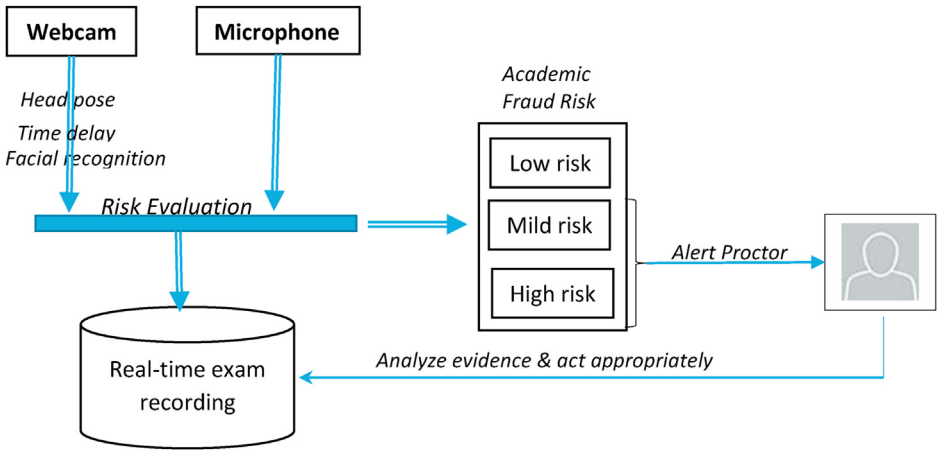

Fig. 3. Continuous monitoring activities.

evaluated for potential cheating as done in Sabbah (2017) so that appropriate action is taken. Once the exam is done, a student can save and submit the electronic answer scripts.

6.2. *Online examination system enablers*

The literature suggests several additional instruments that are critical for the success of an online examination system (Bailie & Jortberg, 2009; Ballentine et al., 2019; McGee, 2013). These include policies; processes; organizational structures; personality traits evaluation and promoting anti-academic fraud attitude; ICT infrastructures; and people, skills and competences. Authors of this study borrowed the terminology in Control Objectives in Information and Related Technologies version 5 (COBIT 5) and view these as "enablers" of online examination systems. COBIT 5 is a tried and tested tool for IT management and governance (De Haes, Van Grembergen, & Debreceny, 2013; Huygh, De Haes, Joshi, & Van Grembergen, 2018). We argue that, if South African universities are to succeed in creating a conducive environment for the management of an online examination system, they should consider these enablers. These enablers are discussed within the context of an online examination system for South African universities.

6.2.1. *Policies*

Study findings suggest that designing and publicizing policies that denounce academic fraud is related to a reduction of academic cheating (McGee, 2013; Paullet et al., 2014; Peled et al., 2018). It is in this regard that South African universities should develop their policies on academic fraud. Ballentine et al. (2019) show a sample of such a policy from a US university. Such a policy should clearly outline what constitutes academic dishonesty or academic fraud, emphasize the need for ethical behaviour and consequences for dishonest (McGee, 2013). These tenants of academic fraud must be constantly monitored, evaluated and reviewed to address emerging threats from new technologies and new ways of committing academic fraud (Amigud et al., 2018). The idea is to identify

new opportunities for commuting academic fraud.

Also, the HEIs should have a policy on how they adhere to international and local privacy laws. There has been an increased requirement for all business institutions that gather personal data to demonstrate how they comply "with privacy and data protection legislation" for example the EU General Data Protection Regulation that was enforced in 2018 (Draaifer et al., 2018, pp. 96–108). South African universities attract students from different continents, hence, it is imperative that if they are to implement online exams, measures should be put in place on the handling of personal data. Such a policy should clearly outline security guidelines to be followed during the storage, transmission and processing of data. For example, RPN is FERPA compliant, a standard that compels universities or remote exam providers to provide strict security measures to personal and exam data (Davis et al., 2016). Furthermore, clarity should be given on the use of data and if any third parties also have access to such data. These measures are expected to address privacy concerns raised by students during online exams (Beust et al., 2018; Lilley et al., 2016; Okada et al., 2019).

Lastly, there is a need to standardize technologies to be used in online exams to guarantee a certain level of performance and avoid unwarranted technical difficulties (Weiner & Hurtz, 2017). For example, outlining the requirements of a desk lamp, minimum recommended internet speed, specifications for computer hardware and webcam (Cramp et al., 2019; Traoré et al., 2017, pp. 73–81; Weiner & Hurtz, 2017). Similarly, Davis et al. (2016) report of quality tests on audio, video and bandwidth. Given the social and economic disparities across race and geographical locations in South Africa, chances are that students may afford different computing that offers different capabilities. For instance, some students may be based in locations where the internet speed is low or may acquire computers that do not meet the minimum recommended specifications. Hence, a policy outline and supportive measures to ensure that students adhere to the recommended guidelines are important.

6.2.2. Processes

Writing an examination is the culmination of several activities that contribute to the overall process. For instance, setting exams, promoting academic fraud awareness, enrolling students, facilitating the exam and evaluating students' performance. The literature suggests that the way online exams should be set is different from that of traditional paper-based exams (Ballentine et al., 2019). There is a general bias towards open-ended questions for online exams as these are not prone to cheating (Vegendla & Sindre, 2019). In particular, Vegendla and Sindre (2019, p. 62) suggest open book online exams with questions based on evaluating "higher levels of knowledge in the Bloom taxonomy rather than low-level recall of facts." The idea is to asses students based on their comprehension rather than their ability to memorize (Ballentine et al., 2019). As such, South African universities should seek to minimize the use of questions that test low levels of knowledge according to the Bloom taxonomy. Where such questions are used, examinees should be made to complete such sections under the pressure of time to reduce the room for searching for solutions elsewhere. Questions that require drawing of diagrams can be accorded more time or be replaced by questions that allow students to draw such diagrams by dragging and combining elements that make a diagram.

Besides, promoting academic awareness is important to address academic fraud. South African universities may consider introducing a compulsory course on academic integrity or ethics to first-year students (Ballentine et al., 2019). First-year students are more likely to cheat or resist online exams because of their lack of experience and knowledge (James, 2016; Okada et al., 2018, pp. 109–122; Woldeab & Brothen, 2019). These challenges are more likely to be pronounced among South African universities given limited access to ICTs and a poor background of rural-based students. Also, procedures to promote the visibility of the academic integrity policy can be considered. South African universities can attach their policies on academic integrity on their websites and course outlines.

Before implementing an online exam system, South African universities should decide on how they will enroll those students who are ready to write the exam. An example was given in Section 3.1.1. Similarly, decisions should be made on how the exam questions should be presented. There are suggestions that a single question should be presented on a page to discourage cheating (MaGee, 2013). Furthermore, the presentation of questions should be randomized. Cramp et al. (2019) give a detailed explanation of how online exam questions can be presented to students to reduce the cognitive burden. Furthermore, all exam sessions should be timed and be available during its specified timeslot. There are recommendations that online exams can adhere to guidelines in the British Standard 23 988 that suggest "that no online exam should last for more than 90 min without a break and, if a longer exam is needed, it should be split into two parts with a break between" (James, 2016). The handling of bathroom breaks should be carefully considered. For example, students may be prohibited from changing answers to questions that were responded to just before going for a bathroom break.

6.2.3. Organization structures

Amigud et al. (2018) suggest the need for clarity on the division of labour among stakeholders when the university is implementing an online exam. Draaijer et al. (2018) share this similar view as they indicated that the structure of universities is not designed in a way that will best suit the administration of online examinations. For example, the roles of proctors need to be redefined that it suits the new exam mode. Similarly, quality assurance teams may need to extend the evaluation of the exam structure to the way it is presented online. Also, staff members to handle activities of student enrolment are also required. Draaijer et al. (2018, pp. 96–108) suggest that new organizational units with own processes will need to be defined. This ensures that the following important questions are answered: who is responsible for the safe storage of the exam once the lectures are done setting? Who should capture the exam on Moodle? Who should maintain access codes for the exam once transferred into the electronic medium? A RACI chart is one of the tools that could be used in outlining roles and responsibilities of those involved in online examinations right from the setting of the papers till the exam is written and exam papers are archived. It simply defines who is Responsible or Accountable or Consulted or Informed about any process that is linked to the online examinations.

6.2.4. Personality traits evaluation and promoting anti-academic fraud attitude

Indications are that personality traits can be used to predict the likelihood of students to commit academic fraud (Peled et al., 2018). For instance, a class where students do not portray the personal traits of conscientiousness, emotional stability, agreeableness, and openness to experience may require strict monitoring during online exams. Also, the attitude of faculty members and students towards online exams may determine their likelihood to engage in fraudulent activities (King et al., 2009; Peled et al., 2018). Thus, the general tone of, for example, management, lecturers, and examinations officers towards good examination ethos may contribute towards the success of online examinations. Tolerated academic fraud or other uses deemed "minor" may set a wrong precedence for students. Hence, faculties need to treat academic fraud as a serious offence. Hosting workshops that promote the awareness of academic fraud is another technique that could be used to make sure that all stakeholders are aware of the university's tone towards academic fraud.

6.2.5. ICT infrastructures

The section on the authentication and monitoring component deliberated on applications that could be used in an online examination system. This section focuses on ICT supporting infrastructures. The importance of the ICT infrastructure is critical as Cramp et al. (2019) noted that Australian universities have to delay the mass implementation of online examinations because of the unequal distribution of ICT

supporting infrastructure. Similarly, an analysis of the South African ICT landscape suggests that sections of the country have a good ICT infrastructure while other sections lack basic structures, especially in the rural areas. Most rural areas have no access to electricity as indicated by individuals who can even go for a week without charging their phones (Bidwell et al., 2013). Access to electricity is equally a challenge for South African rural schools as noted by Mwapwele et al. (2019). Even telecentres that were set up with the help of the government with the intent to offer basic ICTs services suffer from poor internet speed. Gcora, Gopeni, Tuswa, Lwoga, and Chigona (2015) notes of an extremely poor network reception, a problem that has been going on for quite a while, at Cala telecentre based in the rural Eastern Cape Province. Furthermore, a scattered rural population and mountainous terrain make it difficult to install some of these basic ICT supporting infrastructures (Gcora et al., 2015; Rey-Moreno, Blignaut, Tucker, & May 2016, pp. 101–120). In light of these challenges, South African universities can partner with telecentres and schools that have access to ICTs (Gcora et al., 2015) and facilitate their exams through such institutions. This can be done in particular to students who are based in areas where there is poor network reception or no access to electricity. Furthermore, partnering with mobile phone operators for data is another option that could be pursuit by South African universities. However, the biggest worry is that the distribution of broadband and 4th generation technologies remain low in rural areas. This is a huge stumbling block to online examination systems that require an uninterrupted high internet speed to support visual images and text data.

Besides, the United Nations (2018) report shows growing ownership and use of mobile phones among South Africans. However, facilitating online exams requires the use of computers or laptops. The ownership of computers remains low among South African university students. Nearly half of the first-year students (47%) get to have access to a computer for the first time at a university (Oyedemi & Mogano, 2017). This is so because students from a poor background have no access to computers at home and school. As a result, South African universities aspiring to offer online examinations have to seriously ponder on their students' access to ICTs. An alternative approach is to include laptops during tuition so that all students can be given laptops during first-year registration. The universities need to decide on the minimum specifications of laptops to be acquired for students. These laptops can be issued to students with all the necessary software for the exam already installed together with an internet dongle. South African students from a poor background can apply for NSFAS funding that will cover tuition, accommodation, food and stationery. Adjustments to this funding can be considered if students are to be issued ICTs such as laptops and other accessories by the university.

6.2.6. *People, skills and competencies*

Institutions that have implemented electronic exams suggest that ICT skills might be a stumbling block to the success of such a project (Singh & Mansotra, 2015). ICT skills development is important for both the administrators of the online examination system, lecturers and students. In particular, 56% of the first-year students lack basic ICT skills to operate a computer (Oyedemi & Mogano, 2017). South African universities can partner with telecentres and equip students with basic ICT skills to operate computers. First-year students who are based in the rural areas should be given a priority. Besides, South African universities may need to screen those who qualify for the basic ICTs training basing on courses or training that was offered to students while in high school. Students should be taught how to make use of fingerprint scanners, webcams and how to write an online exam. Also, the online examination system should have provisions for trialability such that students can personally assess the online exam environment before the actual exam. Davis et al.'s (2016) RPN provides an example of how this could be done. Similarly, administrators and lecturers need to be equipped with skills of operating an online exam platform. The online platform should be easy to use to promote adoption.

7. Proposed online examination implementation process

South African universities have options to outsource existing online exam systems or develop their own. However, existing online systems may not suit the South African context hence the need to either adopt an existing solution and adjust it according to the context or develop a new solution from scratch. Draaijer et al. (2018, pp. 96–108) observes vendors of online exam solutions in the EU and US. Nonetheless, the implementation process needs to be clearing defined prior to rolling out online exams. This study proposes that South African universities should start by developing policies for online exams. Policies are often the first enabling element that need to be established as these determine how precedures and processes should occur (ISACA, 2015). Hence, South African universities need to align their existing examination policies with the new exam platform and also adopt other unique policies that apply to online exams as highlighted in Section 6.2.1. These policies should adhere to local and international requirements (Draaijer et al., 2018, pp. 96–108). The processes should inform the design of processes to be involved in online exams. These processes are summarized in Section 6.1 and 6.2.2. The designing of processes can be succeeded by the establishment of organizational structures; ICT infrastructures; and the actual development of the online exam system. The online exam system should reflect university policies, processes and procedures. Once the systems are in place, the South African universities should develop measures for personality traits evaluation and promoting anti-academic fraud attitude in accordance to established policies and procedures. Furthermore, all those related to online exams should be given adequate skills that enable the operation of online exams. Fig. 4 shows the proposed implementation process for online exams system by South African universities. Feedback from hosted online exams should be used to continuously inform the design of policies and processes.

8. Discussion and conclusion

This study sought to propose a framework of online examinations for South African universities. As such, the progress on online examination systems was evaluated to propose a suitable solution for South African universities. Long-distance education and the use of online examinations presents an opportunity for South African HEI to find a balance between limited resources and the massification of higher education. This is in line with HEI developments world over (Bailie &. Jortberg, 2009; Barnes & Paris, 2013; Draaijer et al., 2018, pp. 96–108; Okada et al., 2019). However, the biggest concerns on online examinations have been its impact on student performance and the integrity of qualifications given the risk of academic fraud (Amiguda et al., 2016; Ballentine et al., 2019; Cramp et al., 2019; Okada et al., 2019; Paullet et al., 2014; Ullah et al., 2017; Weiner & Hurtz, 2017). Little focus has been paid to other contextual factors of online exams such as the distribution of the ICT infrastructure that saw Cramp et al. (2019) raising questions on the viability of online examinations in Australia. A poor ICT infrastructure in the rural areas together with an unequal society, which has a bearing on the distribution and access to ICTs across the South African society, are some of the major concerns that are expected to complicate the use of online examinations in South Africa. According to the United Nations' 2018 report (United Nations, 2018), only 2.05 per 100 inhabitants had access to fixed broadband in the country. Access to computers is also very limited to university students that are based in rural areas, compared to those that are based in the cities (Oyedemi & Mogano, 2017).

Even though the use of online examinations may cause anxious moments for students, this study findings suggest that the use of online examinations may not significantly affect performance if handled with caution. Indications are that training and the use of online proctors instils confidence and consistent performance across online and paper-based exams, but, failure of which may lead to poor performance in online exams. Furthermore, this study's use of the fraud theory shows that pressure, opportunities and attitude does explain academic fraud

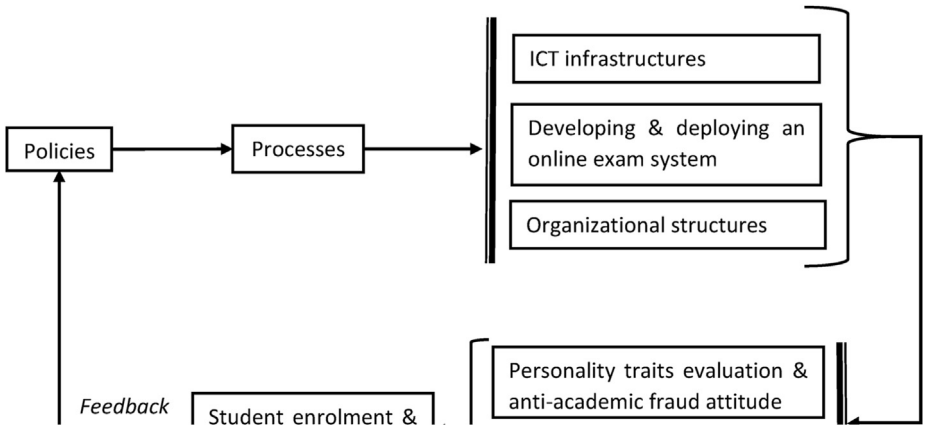

Fig. 4. Online exam system implementation process.

together with personality traits. This has resulted in the proposition of different solutions to fight academic fraud. However, there appears to be a lack of a complete online examination system to combat academic fraudulent activities. This is best demonstrated by the lack of a consensus on what should constitute an online examination system (Chuang et al., 2017; Lilley et al., 2016; Okada et al., 2019; Sabbah, 2017; Ullah·Hannan & Barker, 2019). Besides, the available online examination assessment solutions are not plug-and-play, hence, these solutions will still need to be adapted to their environments (Amigud et al., 2018).

Nonetheless, Apampa and Argles (2010) and Urosevic (2019) suggests that the success of online examination systems lies in the use of biometric-based systems and continuous monitoring during an online exam. Accordingly, this study proposed a holistic online exam framework for South African universities with the aims of finding a balance between the system's impacts on students and preventing academic fraud. By so doing, this study moved away from the practice of proposing techno-centric solutions that are dominant in the literature (Amigud et al., 2018). Such solutions attempt to solve "an Information Systems problem by focusing on technical aspects (technical subsystem) in the hope that the context would adapt to the solution" (Author, 2020), a move that contradicts principles in the Socio-Technical Theory. In steady, this study's framework is based on two modules namely the authentication and continuous monitoring, and online examination system enablers. The authentication and continuous monitoring module focus on student enrollment and standardization, authentication and continuous monitoring. Student enrollment involves the capturing of a student's digital signature based on fingerprints and facial recognition. Students' computer hardware and internet speed will also be evaluated to establish if they meet the recommended minimum requirements. This was necessitated by an unequal distribution of ICTs supporting infrastructure in South Africa. Authentication and monitoring will be done by use of a remote proctor, fingerprints, background sound checks and facial recognition. All these elements can be aligned to the technical sub-systems of the Socio-Technical Theory.

Besides, social sub-systems - as suggested in the Socio-Technical Theory - of this study's proposed framework are explained under the online examination system enablers. These include policies; processes; organizational structure; ICT infrastructure; personality traits and attitude towards academic fraud; and people, skills and competencies. Considering online examination system enablers allows South African universities to contextualize their online examination systems in light of prevailing global concerns around privacy, the need to redefined new business processes, securing new staff members for newly defined roles, balancing the use of online exams across an unequal society and unevenly distributed ICT infrastructures etc. In light of these study findings, it is concluded that the South African HEIs are not yet ready for a wholesale rollout of online examination systems. Short term plans can put more emphasis on alternative forms of assessment such as projects and portfolios (Bailie & Jortberg, 2009; Cramp et al., 2019; McGee, 2013) especially under challenging times of social distancing due to the Covid19 pandemic. Even so, the use of exams remains the most trusted form of evaluating a student's competence. Hence, this study's proposed framework remains useful to the South African universities community as they can use the framework as a point of reference for long term plans to implement online exams.

Declaration of competing interest

We confirm that there is no conflict of interest in writing and publication of this manuscript.

References

Amigud, A., Arnedo-Moreno, J., Daradoumis, T., & Guerrero-Roldan, A. (2016). A behavioral biometrics based and machine learning aided framework for academic integrity in E-assessment. In *International conference on intelligent networking and collaborative systems* (pp. 255–262). IEEE.

Amigud, A., Arnedo-Moreno, J., Daradoumis, T., & Guerrero-Roldan, A. (2018). An integrative review of security and integrity strategies in an academic environment: Current understanding and emerging perspectives. *Computers & Security*, 50–70.

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

Author. (2020). *A model for secure and useable passphrases for multilingual users*. East London: UFH. Thesis.

Bagarukayo, E., & Kalema, B. (2015). Evaluation of elearning usage in South African universities: A critical review. *International Journal of Education and Development using ICT, 11*(2).

Bailie, J. L., & Jortberg, M. A. (2009). Online learner authentication: Verifying the identity of online users. *Journal of Online Learning and Teaching*.

Ballentine, B., Burke, D., Davenport, M., Davis, L., Henderson, B., Irons, J., et al. (2019). *Western carolina university academic integrity task force report*. Western Carolina: Western Carolina University.

Barnes, C., & Paris, B. L. (2013). An analysis of academic integrity techniques used in online courses at a southern university. *Northwest Decision Sciences Institute Annual Meeting Proceedings*.

Beust, P., Duchatelle, I., & Cauchard, V. (2018). Exams taken at the student's home. In *Open and flexible higher education conference*. Aahus.

Bhorat, H., Kimani, M., & Pillay, N. (2018). *POLICY BRIEF. The evolution of national student financial Aid scheme (NSFAS) funding*. Pretoria: LMIP POLICY BRIEF.

Bhorat, H., & Pillay, N. (2017). *The national student financial Aid scheme (NSFAS) and the development of the higher education system in South Africa A description of the demographics and performance of NSFAS beneficiaries*. Pretoria: Labour Market Intelligence Partnership (LMIP).

Bidwell, N. J., Siya, M., Marsden, G., Tucker, W. D., Tshemese, M., Gaven, N., … Eglinton, K. A. (2013). Walking and the social life of solar charging in rural Africa. *ACM Transactions on Computer-Human Interaction*, 1–33.

Bok, D. (2017). How to improve the quality of higher education. Inside Higher ED. Retrieved May 22, 2020, from https://www.insidehighered.com/views/2017/09/21/how-improve-quality-higher-education-essay, 2020.

Chuang, C. Y., Craig, S. D., & Femiani, J. (2017). Detecting probable cheating during online assessments based on time delay and head pose. *Higher Education Research and Development*, 1123–1137.

Cramp, J., Medlin, J. F., Lake, P., & Sharp, C. (2019). Lessons learned from implementing remotely invigilated online exams. *Journal of University Teaching and Learning Practice*.

Davis, N. (2020, March 27). *Maybe the coronavirus will set SA on a path to a more equitable education system*. Cape Town, Western Cape, South Africa.
Davis, A. B., Rand, R., & Seay, R. (2016). Remote proctoring: The effect of proctoring on grades. *Advances in Accounting Education*, 23–50.
De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2013). COBIT 5 and the enterprise goverance of information technology: Building blocks and research opportunities. *Journal of Information Systems*, 307–324.
Draaijer, S., Jefferies, A., & Somers, G. (2018). *Online proctoring for remote examination: A state of play in higher education in the EU. CCIS*. Switzerland: Springer Nature.
Feinman, Y. (2018). Security mechanisms on web-based exams in introductory statistics community college courses. *Journal of Social, Behavioural and Health Sciences*, 153–170.
Ferran, C., González, M. A., Esteves, J., Gómez Reynoso, J. M., & Guzman, I. (2019). AMCIS 2017 panel report: Experiences in online education. *Communications of the Association for Information SysTems, 45*, 433–463.
Gcora, N., Gopeni, A., Tuswa, M., Lwoga, T., & Chigona, W. (2015). The challenges rural women face in using Telecentres: The case of the Eastern Cape Province. In *Proceedings of the 9th IDIA conference* (pp. 84–95). Nungwi.
Hauser, C. (2016). Fees must fall: Anatomy of the student protests in South Africa. The New York Times 22. Retrieved May 22, 2020, from https://www.nytimes.com/2016/09/23/world/africa/fees-must-fall-anatomy-of-the-student-protests-in-south-africa.html, 2020.
Hornsby, D. J., & Osman, R. (2014). Massification in higher education: Large classes and student learning. *Higher education, 67*(6), 711–719.
Huygh, T., De Haes, S., Joshi, A., & Van Grembergen, W. (2018). Answering key global it management concerns through it governance and management processes: A COBIT 5 review. In *Hawaii international conference on system sciences* (pp. 5335–5344). Hawaii: HICSS.
ISACA. (2015). *Cisa - review manual* (26th ed.). Rolling Meadows: ISACA.
James, R. (2016). Tertiary student attitudes to invigilated, online summative examinations. *International Journal of Educational Technology in Higher Education*.
Killourhy, K. S., & Maxion, R. A. (2009). Comparing anomaly-detection algorithms for keystroke dynamics. In *IEEE/IFIP international conference on dependable systems & networks* (pp. 125–134). IEEE.
King, C. G., Guyette, R. W., & Piotrowski, C. (2009). Online exams and cheating: An empirical analysis of business students' views. *The Journal of Educator Online*.
Kuyoro, S. O., Maminor, G. U., Kanu, R. U., & Akande, O. (2016). The design and implementation of a computer based testing system. *Journal of Applied Computation*, 1–7.
Langa, M. (2017). Researching the# FeesMustFall movement. Hashtag: An Analysis of the# FeesMustFall Movement at South African Universities. *Centre for the Study of Violence and Reconciliation*, 6–12.
Lilley, M., Meere, J., & Barker, T. (2016). Remote live invigilation: A pilot study. *Journal of Interactive Media in Education*, 1–5.
McGee, P. (2013). Supporting academic honesty in online courses. *Journal of Educators Online*, 1–31.
McLoughlin, C., & Luca, J. (2002). A learner–centred approach to developing team skills through web–based learning and assessment. *British Journal of Educational Technology, 33*(5), 571–582.
Mohamedbhai, G. (2014). Massification in higher education institutions in Africa: Causes, consequences and responses. *International Journal of African Higher Education, 1*(1).
Mpungose, C. B., & Khoza, S. B. (2020). *Postgraduate Students' Experiences on the Use of Moodle and Canvas Learning Management System. Technology, Knowledge and Learning* (pp. 1–16). Springer.
Mwapwele, S. D., Marais, M., Dlamini, S., & Van Biljon, J. (2019). Teachers' ICT adoption in South African rural schools: A study of technology readiness and implications for the South Africa connect broadband policy. *The African Journal of Information and Communication*, 1–21.
Nader, M., DeMara, R. F., Tatulian, A., & Chen, B. (2019). *Quantitative impact on learning achievement by engaging high integrity testing using lockdown assessment for online delivery*. American Society for Engineering Education.
Ndelu, S. (2017). *A Rebellion of the Poor: Fallism at the Cape Peninsula University of Technology. An analysis of the #FeesMustFall Movement at South African universities* (pp. 13–32). Centre for the Study of Violence and Reconciliation.
Nzimande, B. (2020) Minister Blade Nzimande: Government's intervention measures on Coronavirus COVID-19. South African Government. Retrieved May 22, 2020, from https://www.gov.za/speeches/response-covid-19-24-mar-2020-0000, 2020.
Okada, A., Whitelock, D., Holmes, W., & Edwards, C. (2018). *Student acceptance of online assessment with e-authentication in the UK. Fct.* Springer Nature. htg.
Okada, A., Whitelock, D., Holmes, W., & Edwards, C. (2019). e-Authentication for online assessment: A mixed-method study. *British Journal of Educational Technology*, 861–875.
Oyedemi, T., & Mogano, S. (2018). The digitally disadvantaged: Access to digital communication technologies among first year students at a rural South African university. *Africa Education Review*, 175–191.
Paullet, K., Douglas, D. M., & Chawdhry, A. (2014). Verifying user identities in distance learning courses: Do we know who is sitting and submitting behind the screen? *Issues in Information Systems*, 370–379.
Peled, Y., Eshet, Y., Barczyk, C., & Grinautski, K. (2018). *Predictors of Academic Dishonesty among undergraduate students in online and face-to-face courses*. Computers & Education.
Ramanathan, C., Banerjee, S., & Rao, N. J. (2016). Oaes: Scalable and secure architecture for online assessment and evaluation system. In *IEEE 4th international conference on MOOCs, innovation and technology in education (MITE)* (pp. 296–301). IEEE.
Rey-Moreno, C., Blignaut, R., Tucker, W. D., & May, J. (2016). *An in-depth study of the ICT ecosystem in a South African rural community: Unveiling expenditure and communication patterns*. Information Technology for Development.
Sabbah, Y. W. (2017). Security of online examinations. In I. P. Carrascosa, H. K. Kalutarage, & Y. Huang (Eds.), *Data analytics and decision support for cybersecurity* (pp. 157–200). Cham: Springer International Publishing.
Singh, J., & Mansotra, V. (2015). A cloud based solution for online examination management in education-an architecture. *International Journal of Science and Research*, 1922–1928.
Traoré, I., Nakkabi, Y., Saad, S., Sayed, B., Ardigo, J. D., & de Faria Quinan, P. M. (2017). *Ensuring online exam integrity through continuous biometric authentication*. Information Security Practices.
Ullah, A., Barker, T., & Xiao, H. (2017). A focus group study: Usability and security of challenge question authentication in online examinations. In *International conference on information technology and applications*. Sydney: Academic Alliance International.
Ullah·Hannan, A., & Barker, X. (2019). A dynamic profile questions approach to mitigate impersonation in online examinations. *Journal of Grid Computing*, 209–223.
UNESCO. (2020). Exams and assessments in COVID-19 crisis: Fairness at the centre. Paris, France. Retrieved April 12, 2020, from https://shar.es/aHCJw7.
United Nations. (2018). *United Nations e-government survey 2018. Gearing e-government to support transformation towards sustainable and resilient societies*. New York: United Nations.
Urosevic, K. A. (2019). *Student authentication framework for Online exams outside of school*. Greater Helsinki: Laurea.
Vegendla, A., & Sindre, G. (2019). Mitigation of cheating in online exams: Strengths and limitations of biometric authentication. In *Biometric authentication in online learning environments* (pp. 47–68). IGI Global.
Webbstock, D., & Fisher, G. (2016). *South African higher education reviewed: Two decades of democracy*. Pretoria, RSA: Council on Higher Education.
Weiner, J. A., & Hurtz, G. M. (2017). A comparative study of online remote proctored versus onsite proctored high-stakes exams. *Journal of Applied Testing Technology*, 13–20.
Woldeab, D., & Brothen, T. (2019). 21st century assessment: Online proctoring, test anxiety, and student performance. *International Journal of E-Learning & Distance Education*, 1–10.

Prof T Ngqondi is a Head of School of Computing and Mathematical Sciences and a Chairperson of the Institutional Forum at the University of Mpumalanga. She obtained her PhD in Information Systems at the University of Fort Hare. Her research interest is on Information and Communication Technology with the specific focus on Information and Communication Technology for Development (ICT4D) and Information Technology Governance (ITG). Prof Ngqondi is an active community member who participate on diverse community engagement projects at an individual to national level. Her ambition is to contribute towards human capacity development.

PB Maoneke holds a PhD in Information Systems and an Mcom in Information Systems degree. His research interests centre on cyber security and behavioural information security. Pardon is interested in adopting behavioural science techniques in enhancing end-user privacy.

H Mauwa holds a PhD in Computer Science. He has research interests in ICT4D)-related projects in education, Cybersecurity, Cognitive radio networks, Dynamic spectrum access and Spectrum auction design.