Cape Peninsula
University of Technology

THE DESIGN OF A SOFTWARE ARCHITECTURE SOLUTION TO ADDRESS IMPERSONATION IN ONLINE ASSESSMENTS IN HIGHER EDUCATION

by

STEPHEN MADUVEKO

Thesis submitted in fulfilment of the requirements for the degree

Master of Technology: Information Technology

in the Faculty of Informatics and Design

at the Cape Peninsula University of Technology

Supervisor: Dr B. Kabaso
Co-supervisor: Mrs Denise Lakay

District Six Campus
October 2020

DECLARATION

I, Stephen Maduveko, declare that the contents of this thesis represent my own unaided work, and that the thesis has not previously been submitted for academic examination towards any qualification. Furthermore, it represents my own opinions and not necessarily those of the Cape Peninsula University of Technology.

Signed **Date**

November, 13 2020

ABSTRACT

The advent and accelerated development of computer and Internet technologies have resulted in the simplification, automation and integration of tasks. In education and training, the influence of these technologies includes the introduction and growth of online education and training or eLearning. Parallel to such positive developments caused by these technologies has been the rapid development of novel ways to engage in academic malpractices or cheating such as plagiarism from online and electronic sources, collusion or unauthorized collaboration, and impersonation. The eLearning mode of education means that there may be no physical contact at all between the provider and consumer of education. This mode allows educational transactions to happen over a physical distance. This separation can result in the student being an anonymous entity within the system. Academic fraud has drawn much attention as it threatens to undermine the credibility of online qualifications and assessments. This study was on the challenge of student impersonation and the authentication technologies that can be used against impersonation. Stakeholder concerns were solicited and various authentication technologies explored to design a software intensive, architectural solution that could reduce impersonation in online assessments. The research revealed the prime challenges faced by current anti-impersonation measures. The challenges faced include cost issues such as the acquisition of new hardware, the threats to personal data, data security and threats to privacy. This knowledge provided a foundation for the design of a software architecture for a secure online assessment system that can reduce impersonation. The low-cost solution would not demand new hardware implements beyond the basic configuration of a personal computer. The research employs a mixed method approach to solicit the concerns of stakeholders in online Higher Education assessments. The product of the research is a proposed software architecture description of a secure online assessment system that reduces impersonation. The proposed architecture combines different types of authenticators to deliver a “technologically secluded” student assessment environment. This proposed online assessment system is effective in reducing impersonation, is not expensive as it only requires basic computer hardware, and is less intrusive than other existing online assessment security systems .

ACKNOWLEDGEMENTS

I wish to thank the following persons for their valuable contributions towards the delivery of this thesis:

My wife and my children for their encouragement and motivation.

My workmates and colleagues in academia; N. Botha, R. Mavhunga, L. Carolus, S. Samusodza, I.S Musakwa, M. Jin, S. Lombard, O. Dyantyi, R. Mee, T. Mlambo, N. Chigaba, G. van Dieman, G. Delport and C. Watambgwa.

Dr. Mugari, Dr Brand, Messrs. T and K. Rioga, Israel, Goodman, for the valuable discussions and arguments, you shaped my thoughts and approach.

Dr. Museka and all the staff at the Institute for Research and Development (Mbabane) for the answers and the questions too!

Ms S. Mitchel who went the extra mile to make this product readable.

My supervisors, Dr. Kabaso and Mrs. Lakay for guiding me and providing a roadmap to completion of this task.

I extend a hearty “thank you” to Mrs. Naseema Allie who made this document a readable thesis.

The financial assistance of the University Research Fund towards this research is acknowledged. Opinions expressed in this thesis and the conclusions arrived at, are those of the author, and are not necessarily to be attributed to the University Research Fund.

DEDICATION

To my wife and children, for all the love and everything else that I ever needed.

ABBREVIATIONS & ACRONYMS

Abbreviation	Expansion / Explanation
ACK	Acknowledgement
ANN	Artificial Neural Network(s)
API	Application Programming Interface
A/V	Audio Video / Audio Visual
GPS	Global Positioning System
ICT	Information and Communication Technology
IMS	Identity Management System
LMS	Learning Management System
OTP	One-Time Personal Identification Number / One-Time Password
PIN	Personal Identification Number
SMS	Short Message Service
TCP/IP	Transmission Control Protocol / Internet Protocol

GLOSSARY

Term	Definition/Explanation
Academic fraud	Any act that violates the rules, protocols, values and regulations that govern education and educational integrity.
Assessment	Methods or tools used in formal education to measure, determine the learning progress, academic readiness, skill acquisition, or educational needs of students.
Authentication	Processes by which identity is established, confirmed and verified through the collection of data and confirmation that the person is who they claim to be.
Authorization	The act of granting permission to do something. Authorization also specifies what data the object is allowed to access and what the object can do with or on the data.
Identity	The information that states who the bearer is. It is the basis of establishing the validity and admissibility of an individual.
Impersonation	An act of pretending to be another person for some gain e.g. financial gain.
Online assessment	Assessment that takes place in the presence of a network connection between the student and the facilities that deliver the assessment.
Software	The programmed instructions that make computers and other systems work in a certain manner to achieve a defined objective.
Software architecture	An assembly of components, their characteristics and behaviour that defines the function and features of a software-based system.
Third party	Any person(s) besides the registered student who engages in an academic activity where a registered student is required or expected.

TABLE OF CONTENTS

CHAPTER ONE
INTRODUCTION

1.1 Overview

Commencing in the 1990s, the use of Information and Communication Technologies (ICTs) continues to cause changes in human activities. Business and commerce, entertainment, leisure and relationships have undergone change under the influence of these technologies (Goodman-Deane et al., 2016; Chen & Karahanna, 2018).

Change has also been experienced in education and training where teaching, learning and assessment processes have undergone drastic change (Mayer, 2019). One example of the changes experienced in education is the advent and growth of eLearning (Asha & Chellappan, 2008). Asha and Chellappan (2008:1) present eLearning as

"…a new form of learning that is becoming more and more popular everyday".

Tikam (2016:25) concurs and points to the rapid computer-driven evolution that is taking place in the face-to-face classroom environment as a driver to change in the entire landscape of education. Tikam (2016:25-26) highlights electronic learning or eLearning as a viable alternative to 'conventional' face-to-face education. eLearning avails new educational opportunities to people the world over. Allen and Seaman (2013: 24) characterize eLearning as a mode of education that affords students opportunities to learn "whatever, wherever, and whenever" allowing them to do what work they choose, at any time, pace and at any place of their choosing.

As is the case in all modes of education, assessments form the main tool used to measure achievement in online education or eLearning (De la Orden, 2011; Onyibe, Uma & Ibina, 2015). The authors point out that assessments at Higher Education level provide gateways or entry to employment and other opportunities because the outcomes or results generated by assessments have a clear impact on the lives and development of individuals, families, local and global communities. Akintunde and Selzing-Musa (2016:110) emphasize the value of assessments in higher education and label assessments as the "bedrock upon which an individual's future achievements depend".

Akintunde and Selzing-Musa (2016:112) are of the opinion that among other factors, the emphasis placed on assessments as a major determinant for qualification and completion, places students under pressure to succeed. The authors elaborate that this pressure leads some students to fraud or cheating in the hope of performing well in those assessments.

Daumiller and Janke (2019) indicate that society and business suffer immensely when they are denied the benefits expected from quality graduates that the education system should deliver because of examination misconduct, cheating or academic dishonesty. Akintunde and Selzing-Musa (2016: 110) sums up the negative impact of academic cheating as a hindrance to the effectiveness of the entire education process; by de-establishing the necessary evidence of learning or skill acquisition.

Seeking unfair, illegitimate assistance or representation from third parties during assessments is one of the many ways in which students cheat. This type of cheating is called “impersonation” (Watson et al., 2010). The authors defined impersonation in education as the fraud that happens when a person, other than the student, participates in studies or assessments in the place of the registered student.

The Oxford Living Dictionary (2018: online), defines impersonation as “…an act of pretending to be another person for the purposes of fraud”. In Higher Education, ensuring the legitimacy of the person taking the assessment is essential in order to maintain academic integrity and uphold the values of the qualification, awarding body, institution, and industry integrity (Peytcheva-Forsyth & Aleksieva, 2019:1872).

Legal means have been engaged in the fight against academic fraud. For example, Brimble (2016), cites the American Higher Education Opportunity Act (HEOA) of 2008 on the need to fight academic offenses, focusing on the offense of impersonation. The HEOA (2008) states that:

> “Institutions that offer distance education must have processes through which they establish that the student who registers for a distance education or correspondence education course or program is the same student who participates in and completes the program and receives academic credit.”

The EMA (2012:2) defines academic malpractice as:

> "Any act of commission or omission by a person who in anticipation of, before, during, or after any examination, contravenes the rules and regulations to the extent of undermining the validity, reliability authenticity of the examination and ultimately, the integrity of the outcome given."

The HEOA (2008) and the EMA (2012) are examples of legal instruments that compel Institutions to install mechanisms that ensure the provision of a virtual learning environment that can only be accessed by legitimate students, monitoring and tracking of students' learning activities and adequate mechanisms to deter and detect academic misconduct in various forms such as impersonation centrally.

The HEOA (2008) demands authentication mechanisms in online assessments that reduce academic offences including impersonation. In addition, McNabb (2010) argues that technologies that can continually monitor the student during an assessment are ideal for credible online assessments.

Underwood and Szabo (2003) and Adil, Simon and Khatri (2019) attempt to quantify the challenge of impersonation in online education. The authors focus on the need for conclusive means of identifying and authenticating students taking assessments. Many novel methods such as biometric technology have been developed to fight impersonation. Lee-Post and Hapke (2017) compare technologies such as passwords, tokens, facial recognition, motion detection and video recording, pointing out that these methods all have some weaknesses and tend to be either intrusive or minimally robust. Current research projects share the common aim of securing online assessments through identification and authentication of assessment takers while causing minimum disruption during the assessment (Peytcheva-Forsyth & Aleksieva, 2019: 1872; Av & Rathi, 2019:184).

The researcher believes that a software architectural solution for online assessment systems will increase the security of online assessments by discounting illegal participation by third parties. This research aims to design a software architecture for a secure online assessment system that is non-intrusive and discounts impersonation.

1.2 Background to the research problem

De la Orden (2011: 2) recognize that academic institutions compete in the provision of an essential service to society. They argue that institutions are compelled to distinguish themselves and prove that they do so, by some formally recognized assessment mechanism. Failure to achieve this requirement can harm their reputation and cause problems with recruitment, enrolment, and even accreditation (Keil & Brown, 2014:15).

Rowe (2004) generalizes that, to a large extent, accurate assessment methods help to insure the survival of educational institutions. De la Orden (2011) observes that the Higher Education system uses assessments to measure progress and gather evidence of learning, knowledge or skills transfer. This is supported by Tikam (2016) who found evidence that achievement at Higher Education level is measured in terms of performance in final assessments. These authors highlight the necessity for achievement or successful completion of a course, as a symbol for recognition. Tikam (2016) conclusively shows the high value of co-existence between achievement and assessment, which justifies why education must include assessments.

Kinoti (2015) adds that using assessments as an evaluation tool provides academic institutions with a means of determining the student’s knowledge, skills and abilities, explaining why results from assessments are used in employment and other decisions in business and society. The authors pondered on the societal impact of graduating incompetent individuals and mentioned the losses and dangers that such persons would cause on society. They cited for an example, the deployment of incompetent individuals to serve communities. Kinoti et al. (2015) agrees with De la Orden (2011) that in order to succeed in Higher Education, students need to demonstrate various skills and abilities by performing well in formal summative assessments.

McCabe, Trevino, and Butterfield (2001) argued that summative assessments at Higher Education level could pressure students to cheat with the hope of achieving higher grades. McCabe, Trevino and Butterfield (2001) note that because students value high grades and successful completion of Higher Education assessments as passports to progress in the business and industrial world, students may seek success at very high costs and risks. Hence the conclusion drawn by Lang and Hayford and Lang (2013:82), that:

> “cheating and Higher Education … have enjoyed a long and robust history together.”

The high value placed on success in summative assessments in Higher Education to measure success and determine completion, explains why summative assessments are considered "high stake "assessments. This explains why it is essential for institutions to implement adequate security controls in academic assessments (James, 2016). Higher Education institutions are entrusted to ensure that students receive academic awards, recognition and rewards that are a truthful reflection of their level of performance or potential (Cluskey, Ehlen, & Raiborn, 2011).

It is a fundamental institutional requirement to ensure that students receive academic awards when they achieve the best grade possible. For some students, this means getting good grades by all means possible. As McCabe, Trevino and Butterfield (2001), De la Orden (2011) and Kinoti (2015) conclude, this "conflict" sometimes leads some students to engage in various endeavours targeting finer achievements; some of which tend to be outright fraudulent.

Over the past twenty years, research has confirmed the fact that some students engage in various malpractices to cheat in assessments. This research has confirmed the fact that some students engage in various malpractices to cheat in assessments (e.g. Rowe (2004); Weippl (2005); Kinoti et al. (2015); Mahesh and Selvajyothi (2017) and Mellar, Harvey and Peytcheva-Forsyth (2018).

Busayo (2008:28) defined examination or assessment malpractice as follows:

"an improper and dishonest act associated with examination with a view to obtaining an unmerited advantage".

Academic dishonesty is a serious concern and according to Bruno and Ibidigbo (2012), academic dishonesty can render an examination ineffective and useless. Bruno and Ibidigbo (2012) elaborate that the dishonesty may be on the part of any stakeholder such as educational administrators, teachers, parents or students.

Rowe (2004), Pillsbury (2004), Weippl (2005), Kinoti (2015), Mahesh and Selvajyothi (2017) and Mellar et al. (2018) all underscore the pervasive need to safeguard and ensure academic assessments from all dishonest behaviour from students and other players. Peytcheva-Forsyth and Aleksieva (2019) agree with Cronan, McHaney, Douglas and Mullins (2017) concluding that assessments in Higher Education are of primary importance in keeping the outcomes and qualifications acceptable, credible and valuable to both academia and industry. Ensuring the legitimacy of the person taking the assessment is essential in order to maintain academic integrity.

The authors argue that the value and recognition accorded to academic success take meaning when academic awards and rewards are given to individuals who have actually undertaken study in the given area of specialty and show competency or knowledge through assessment. Mellar et al. (2018) charges institutions with the responsibility to safeguard the integrity and value of the qualifications they churn out.

It can be noted from the above discussion that ideally, assessments ought to be taken only by persons officially known by registration at the institution, such that the award is accorded to the correct individual. Hayford and Lang (2013) established that students tend to engage in malpractices of different forms such as impersonation, targeting higher grades in the end. The authors continue to submit that impersonation in education breaks the relationship between the ability, knowledge or skill set of the person, and the expectations of the qualifications bestowed upon them by academic institutions. According to Styron and Styron (2010), through impersonation, work done by third parties gets recognition in the name of the legitimate student.

Numerous studies (e.g. Gathuri, Luvanda and Matende, 2014; Tikam 2016; Mellar et al., 2018; Adetunji et al., 2018) present the benefits resulting from the growth of online education and online assessments. Researchers show online methods as viable alternatives to 'conventional' education and assessment methods. The authors all include the potential of eLearning to avail hitherto impossible educational opportunities to many people, regardless of their physical location, age or lifestyle. Fisher et al. (2016), expresses worry that the novel uses of technologies bring with them not only new possibilities, but also new motivations and means to students to cheat through applications of technology e.g. plagiarism from online sources and impersonation.

Much research has gone into developing ways of increasing technology usage in academic assessments while reducing academic dishonesty by identifying, authenticating and monitoring students during assessments (for example Agulla, Castro and Mateo 2008; Apampa, 2009; Ullah, Xiao and Lilley (2012); Akintunde and Selzing-Musa, 2016; Abnave, Banaiti and Chopade, 2017; Adil et al., 2019). In summary, such research has led to the development and utilization of security technologies in online assessments.

The technologies range from simple username and password pairs to advanced biometric controls (O'Gorman, 2003; Okada, Whitelock & Holmes, 2019); Omolara, Jantan and Abiodun, 2019 and Hedaia, Shawish and Houssein (2020). A common characteristic of these solutions is the need for new hardware or software to be acquired and installed to enable student identification and authentication during assessments. The 'basic off-the-shelf' computer may be insufficient for satisfactory use in online assessment and extra equipment or software is necessary (Oreilly & Creagh, 2016; Onyema et al., 2019). The authors agree that such additions raise the cost of online education and assessments and students have to bear the costs of their education.

1.3 Motivation

My twenty-five years of experience as an educator, facilitator and involvement in industry-based training revealed to me many facts. This includes the evolution of training technologies, the value students place on success and also the ways in which students attempt to cheat in their quest to succeed. I have also gained an understanding of why institutions take an interest in keeping their assessment systems secure from the threats of students cheating. Of particular interest to me were students' performances in various assessments over the duration of their studies. My attention was especially drawn to the introduction and growth of eLearning, and why online assessments affect student performance (Kinoti, 2015; Alammary, 2019).

As an assessor at tertiary education level, participating in distance education, I observed that the achievement of some students in face-to-face or invigilated assessments varied greatly in comparison to assessments that were not invigilated or submitted online on Learning Management Systems. I had a strong suspicion that some of the students got the online assessments done by others and thus sought explanation for my observations. In order to achieve this, I studied impersonation in detail with the intention of understanding impersonation it well enough to make some contribution towards the reduction of impersonation in academic assessments at the Higher Education level.

1.3.1 Pre-study

Following the preliminary review of existing research, a pre-study was performed at two online assessment centres using three basic methods. The researcher used the pre-study to establish the following:

i. Researchability: The researcher was keen to test the research idea and determine if the research could possibly be taken and completed subject to time, cost and other material constraints. The researcher was keen to determine the availability of data for the research process from stakeholders in online assessments.
ii. Fit: The researcher needed to determine gaps in existing knowledge.
iii. Formulate a formal research statement and research questions: The researcher needed to crystallize the research idea into a clear research statement and set of concrete research questions.

To obtain the information necessary to establish each of these objectives, the researcher employed the following procedures:

a) A pilot round of interviews and formal discussion with faculty members, two academic quality managers, one assessments manager and two assessment centre managers. The pre-study primarily aimed at obtaining some insight into these participants' understanding and knowledge of impersonation and the extent of the challenges it posed.

b) A literature review guided by the key points obtained from the discussions was done to enhance the researcher's understanding of impersonation in the online assessment setting, and how educational practitioners and institutions were coping with impersonation.

c) The researcher observed faculty team members as they setup and administered online assessments.

By studying available literature, observing online assessments as they took place and held extensive discussions with colleagues and other subject-matter experts, the researcher realized a need to conduct a formal research into how online assessments can be made more secure against impersonation. The researcher had questions around how assessments could be secured with minimum hardware and software costs, how this could be achieved without causing disruption to the student taking the assessment, and how existing technologies could be harnessed for use in online assessments. These questions were gradually refined into the formal research questions.

Following the pre-study, the researcher sought the consent of two academic institutions for the conduct of formal research into online assessments at Higher Education level. This research focuses on the design of a cost-effective assessment system that can discount impersonation in online assessments without disrupting the student's experience.

1.4 Statement of the research problem

The literature review revealed that the Learning Management Systems (LMSs) available today provide comprehensive online education facilities. However, they do not seem to provide the level of robustness necessary to conclusively ensure that the registered student takes the online exam themselves, or even determine if the correct student spends the whole assessment session in front of and working the computer. Apampa (2010) emphasizes the need for adequate authentication of the student, not only at the start, but also throughout the assessment, to ensure that the same student participates throughout the process. Security shortcomings in assessment systems impose challenges on the credibility and integrity of the assessments. Legislation such as the Higher Education Act (2008) and the Examination Malpractice Act (2012) raise the need for academic integrity, challenging institutions of Higher Education to install adequate authentication mechanisms in online assessments to fight impersonation.

Efforts to restore or raise the credibility and integrity of online assessments are necessary. These efforts must focus on improving online assessments to the extent that access to the assessments and the information captured or generated during the assessments and transmitted across the entire system is safeguarded against various forms of impersonation.

The research problem targeted by this research is the absence of comprehensive defences against impersonation in online assessments taken at Higher Education level (Prince et al., 2009; Rodchua, Yiadom-Boakye & Woolsey, 2011); Karim & Shukur, 2017; Abnave et al., 2017).

1.5 Aims and objectives of the study

This research aims to develop a software architecture for online assessment systems that reduces impersonation in formal online assessments at Higher Education level. The objectives of this research are to:

a. identify ways by which impersonation happens during online assessments.
b. design a software architecture that can reduce impersonation during online assessments.

c. evaluate the suitability of the designed software architecture in terms of different stakeholder interests, for instance the cost, performance, and usability (including end-user experience).

1.6 Rationale of the study

The need to correctly identify and authenticate students in online assessments is central to the provision of credible academic credits and qualifications (Adil et al., 2019). King and Case (2005) reveal that students believe that it is easier to cheat in online assessments and that cheating is common among students in all forms of assessment. King and Case (2005) argue that detective and preventative controls are necessary to minimize e-cheating in particular. Many technologies have been developed to safeguard online assessments e.g. passwords, tokens and biometric controls (O'Gorman, 2003; Lee-Post & Hapke, 2017; Peytcheva-Forsyth & Aleksieva, 2019). Pervasive in these works is the realization that students will, if chance avails engage in dishonest behaviour such as plagiarism and impersonation should the opportunity arise.

The rapid growth in online education has made education more accessible by globalizing the reach of academic institutions (Allen & Seaman, 2013; Mayer, 2019). The accelerated growth of online education has resulted in the 'any time and any place' availability of education and assessment through Massive Open Online Courses (MOOCs) and the development of paperless online transactions (Allen & Seaman (2013).

The growth in online education has also been associated with the increase in online and computer-based education is the increased ease with which students can engage in dishonest acts (Akintunde & Selzing-Musa, 2016). Daumiller and Janke (2019) indicate that society and business suffer immensely when they are denied the benefits expected from quality graduates that the education system should deliver because of examination misconduct, cheating or academic dishonesty.

Various methods have been developed to curb or reduce incidences of academic practices such as impersonation using identification, authentication and monitoring technologies (Apampa et. al., 2010). The technologies include username and password pairs (Zviran & Erlich, 2006), token based authentication that use an object assigned to the legitimate person for authentication purposes (Velasquez et al., 2018)., biometric controls (Karim & Shukur, 2016; Seo & Wyrwas, 2019; Raul et al. (2020) and predicative technologies such as the tracking of physical location, the hardware used during the assessment and behavioural patterns (Lee-Post & Hapke, 2017).

Each of these technologies has its own merits and potential areas of usage. However, a common shortfall among the majority of these technologies such as token-based authentication, biometric authentication and predicative authentication is the need for extra hardware and software to be utilized. The burden is increased when the sensitivity of the equipment, such as scanners are taken into account (Chuang, Craig & Femiani (2017) 2017; Omolara et al., 2019).

This research acknowledges the developments in information and communication technologies such as the increased availability of compact, more affordable high grade servers, the availability of high quality Learning Management Systems (LMS), the increased availability and utilization of cloud and fog computing online education jointly make hosting online education services more feasible for most institutions. This research's point of departure is that the costs of the service end upon the shoulder of the student. For instance, the costs of hardware, software and other implements are either factored into the fees payable by the student or the student left with no choice but to use its own means to have the implements and technology available for their use.

Focusing on accessing secure online assessments, this research targets to propose a software architecture that can interface with the LMS that hosts the assessments (on institutional hardware) using standard and small computer devices including laptops, palmtops and tablets that have limited storage and other specifications. This research is premised on the assumption that the software that drives the entire assessment process runs off the institution's hardware and does not require high – end equipment on the part of the student.

It is envisaged that in such an architecture, the student can take assessments from any place, at any time and on any hardware that can access the Internet and the LMS. The significant outcome of this architecture is the provision of secure online assessments at a reduced cost on the part of the student who has the added benefit of using any available computer.

1.7 Research question

How can online assessment systems be designed at the architectural level to reduce impersonation without imposing extra hardware costs to the institution or end-user?

1.7.1 Research Sub-Questions

SQ1: What measures do current online assessment systems implement to counter impersonation?

SQ2: To what extent are the current online assessment systems succeeding in countering impersonation?

SQ3: What features should a software architecture define in order to counter impersonation in an online assessment software system?

SQ4: What performance metrics are required to evaluate a software architecture?

1.8 Significance of the study

This research will inform the design of secure online assessment systems to reduce impersonation.

This research contributes towards encouraging fair academic practice among online students. Further consideration and implementation of the knowledge and options revealed by the research should assist in improving the designs of online qualifications and assessment systems. The findings may provide information for further research in academic assessment malpractices.

1.9 Delineation of the study

The research focuses and limits its attention to understanding academic impersonation in online assessments with the aim to design of a software architecture that reduces impersonation in online assessments. Other types of assessment academic offenses are considered only in reference and comparison against / to impersonation in online assessments.

The research employs a mixed method approach to solicit the concerns of stakeholders and enhance the researcher's understanding of academic impersonation and existing counter measures using two registered Higher Education institutions. Structured interviews, literature / document reviews and direct observation are the tools used to collect data from stakeholders and online assessment events. Qualitative data analysis based on thematic analysis of stakeholder interview feedback and inductive reasoning and techniques were used to analyse the data collected.

The study is restricted to providing a specification of the architecture which does not include actual implementation of the proposed software architecture in real life. The definition of this project’s scope is based on the assumption that the key non-functional requirements of a Learning Management System (LMS) used in online Higher Education include performance, availability, reliability, security and maintainability (Voas, 2004). Table 1.1 summarizes the views and the non-functional requirements of an LMS in the form of a matrix. Sections 1.9.1 and 1.9.2 provide details of the project’s scope in line with Table 1.1.

Table 1.1: Views and non-functional requirements (adapted from Voas, 2004)

Viewpoints	Non-functional requirements						
	Security	***Performance***	***Availability***	***Evolution***	***Flexibility***	***Responsiveness***	***Administrability***
Operation	Operational security	Operational performance	Operation availability	Operation evolution	Operation flexibility	Operation responsiveness	Operation Administrability
Concurrency	Concurrency security	Concurrency performance	Concurrency availability	Concurrency evolution	Concurrency flexibility	Concurrency responsiveness	Concurrency Administrability
Information	Information Security	Information performance	Information availability	Information evolution	Information flexibility	Information responsiveness	Information Administrability
Functional	Function Security	Functional performance	Functional availability	Functional evolution	Functional flexibility	Functional responsiveness	Function Administrability

1.9.1 Inclusions

Online assessments make extensive use of both information and communication technologies. According to Rosenberg (2011), there are two major security areas in online assessments namely, information security and operational security.

1.9.1.1 Operational security

Rosenberg (2011) defines operational security as the way in which the system safeguards stakeholder interests, reduces or prevents abuse, such as illegitimate access and use of its resources, exchanging, storing and updating system components, and procedures or processes. In this context, resources mean the courseware, correspondence, stored data, data in transmissions, and the assessments hosted on the LMS.

1.9.1.2 Information security

According to Rosenberg (2011), information security describes the way that the system provides for information creation, secure storages, manipulation, management, containment and its secure distribution; safeguarding against impersonation or adulteration of data pertaining to legitimate students by inputs from illegitimate agents. It is anticipated that the proposed architecture that focuses on these two aspects of security will fit into the enterprise architecture for a Higher Education institution assessment as a subsystem. This means that the proposed architecture will be treated as a component of the enterprise architecture and it will be focused on addressing the issues of informational and operational security in online assessments only. This research adopts the definition of Alruwais, Wills and Wald (2018:12) for online assessments as follows:

“an evaluation of a person’s abilities, behaviours and/or characteristics using the Internet or other available computer technology.”

This research therefore does not consider take-home assessments that may be submitted electronically as “online assessments” because the student does the actual work in the absence of a connection to the assessment system or even a computer network – technically making the assessment “offline” (Bal et al., 2011). Attention is limited to assessments that happen in the presence and persistence of an electronic pathway connecting the student to the assessment system.

1.9.2 Exclusions

Rosenberg (2011) argues that commercially available Learning Management Systems (LMS) that host Higher Education assessments adequately deliver the functional and concurrency security requirements. This research takes this argument into account and does not cover function and concurrency security, leaving, as proposed by Rosenberg (2011), these to be satisfied by the Learning Management System. This research's focus is on the operational and information security requirements of online assessment systems as highlighted in Table 1.1.

1.10 Ethical considerations

The nature of this research demanded the researcher to interact with various stakeholders, such as students, parents, institutions and faculty staff. It was imperative for the researcher to enter into the "personal space" of the stakeholders and access sensitive information and viewpoints. Participation in the research activities was completely optional and no participants were coerced either by the researcher, parents or management. For these reasons, the researcher sought and obtained ethical clearance from the institutions from which participants were drawn.

Obtaining clearance followed formal discussion and agreement with management of the scope and depth of the research, the research methods and the manner in which the derived information would be utilized, communicated, stored and disposed of after use. Pre-engagement announcements were made in the institutions by management to give potential participants the opportunity to choose whether or not to participate. Discussions with participants were utilized prior to engagement in the process of data collection to provide clarification on matters such as the right to remain anonymous, the guarantee that no harm would befall the participants. The methods by which findings would be disclosed or manner in which the data was to be used and ultimately disposed of were clarified. All participants had the right to withdraw from the project at any time with no questions asked.

For students below the age of 18 years, parental consent was obtained prior to engaging the student in the research. All students had the option of being interviewed in the presence of their parents. Three of the interviews with students were conducted in the presence of the parents.

The researcher pledged and upheld the guarantee that no person, individual or organization was coerced to participate in any activity during the research process. The guarantee specified that all the data and artefacts that the project collected would solely be used to serve an academic purpose. The researcher ensured that all the results that were obtained from the analysis of collected data was reported, provided “as is” with no alteration, adjustment or bias, and further guarantees that no physical, psychological or emotional harm befell any participant because of the research and its outcomes.

For confidentiality and stakeholder safety, all data gathered (i.e. audio recordings, notes and other documents) from these tools was transcribed and stored in an encrypted format on a password and encryption secured laptop and thumb drive.

Finally, the researcher undertook to ensure that the conclusions drawn from the research are only available through channels and on platforms that the CPUT expressly authorizes. All artifacts, hardware and software used in the research were licensed to either the researcher or CPUT.

1.11 Chapter Summary

Chapter One introduced the problem of impersonation in online assessments. The chapter provided the background, the justification for the study, and the aims and objectives of the study. Further, the chapter presented the research questions and significance of the study, the study’s delineation, and the ethical considerations of the study. Chapter Two focuses on understanding, collating and analysing previous research works to develop a context for this study.

CHAPTER TWO
LITERATURE REVIEW

2.1 Overview

For this thesis, a systematic literature review structured according to Kitchenham, Pretorius and Budgen (2010) gave insight into the nature, the challenges posed by academic dishonesty and the progress made in the fight against academic dishonesty, such as impersonation. The review explored the various types of assessments used in Higher Education and the reasons students engaged in academic malpractices. The methods that students commonly applied in academic cheating and the measures implemented in online assessment systems by institutions to prevent or detect the malpractices were also revealed during the review.

Chapter Two aims to present a literature review to provide an informed understanding of academic offences focusing on impersonation in Higher Education and show how impersonation happens during online assessments. The Chapter summarizes the literature review into how existing online assessment systems fight impersonation and the Chapter also explores the implications of the findings in the fight against impersonation in online assessments. The chapter concludes with suggestions to use system engineering approaches to design a software architecture that can reduce impersonation in online assessments.

2.2 Approaches to Higher Education

Higher Education takes various forms, the prime of which are face-to-face or “classroom education” and “distance education” (Rowe, 2004). The various forms that education and assessments take in Higher Education are described as follows:

2.2.1 Conventional or face-to-face learning / education

The conventional model of education is one in which the educator and the student make physical contact for teaching, learning, consultation and assessment purposes. In this form of education, the teacher is considered a “reservoir” of knowledge and skill and the student a “receptacle” to which the knowledge and skill must be transferred (Rowe, 2004). Moore and Kearsley (2012) submit that in the face-to-face education, the teaching and learning activities happen synchronously i.e. at the same time and the teacher and student become acquainted with each other over time. Bohnsack and Margolina (2019) emphasize that the student has very little control over what content they learn, when they learn it and the pace at which content is discharged. They explain that this is because face-to-face education adheres to strict time and place constraints, the objectives and the schedule of the teacher. Bohnsack and Margolina also describe face-to-face education as learning confided to a “brick-and-mortar” physical environment.

2.2.2 Distance education

Moore and Kearsley (2012:4), explain distance education as follows:

“Distance education is teaching and *planned* learning in which teaching normally takes place in a different place or time from learning, requiring communications through a combination of technologies such as mail correspondence, audio, video, computer and the Internet and special institutional organization”.

According to Simonson (2018), distance education is an educational paradigm that leads to several benefits such as increased access to learning and training matter, and an increase in the capacity of the educational system. Moore and Kearsley (2012) indicate that the distance education model has the potential to conduct the education transaction with the teacher and student not reaching a point of complete familiarity or acquaintance. Alammary (2019) describes distance education methods as those that breach the time and distance constrictions that face-to-face imposes on education.

2.2.3 Online learning / education

Allen and Seaman (2013:7) present online education as:

“a modern version of distance education which uses computers and the Internet as the main methods of delivery with at least 80% of content delivered by these electronic technologies”.

Allen and Seaman (2013) suggest that online education and assessments require a different pedagogy as online education systems break down the barriers of time and place imposed by traditional education. Allen and Seaman (2013) indicate that this is necessary to enable teaching, learning and assessment of students to take place without physical contact or time synchronization between the student, institution and educator. Baleni (2015) submits that the aspect of time and physical geographical separation makes online assessments usable in distance education. Bell and Fedeman (2013) clarify the distinction between distance and online education basing on the extensiveness of information technology and the time variance between teaching and learning activities. The authors argue that in distance education, teaching and learning are asynchronous i.e. they do not happen at the same time. They contrast teaching and learning activities in the online learning model where the process can happen at the same time via modern technologies such as instant messaging, web chats, social media, live video and the telephone or not at the same time through recorded video, podcasts and other digital media.

2.2.4 Blended learning / education

According to Bohnsack and Margolina (2019), blended learning incorporates traditional face-to-face classroom methods of instruction with computer mediated activities from digital media or online sources, thereby creating a blend or mix of learning experiences applicable even to distance and correspondence education. Alammary (2019) adds that blended learning differs from face-to-face learning in that the student has a level of control over the time, place, path and pace at which learning takes place.

2.3 The ecosystem of assessments in Higher Education

In efforts to measure student progress and achievement, academic institutions employ various types of assessments. At a high level, assessments in Higher Education may be low or high stake in value, closed book or open book by nature. Alternatively, assessments may be classified as formative or summative when considering timing and content of the assessment. Other classifications identify assessments as non-invigilated or invigilated, online or offline, knowledge-based or competency / skill based.

Figure 2.1 shows a summary of the ecosystem of assessments in Higher Education. The different forms of assessments overlap extensively, but Figure 2.1 and the descriptions below attempt to show how they individually differ.

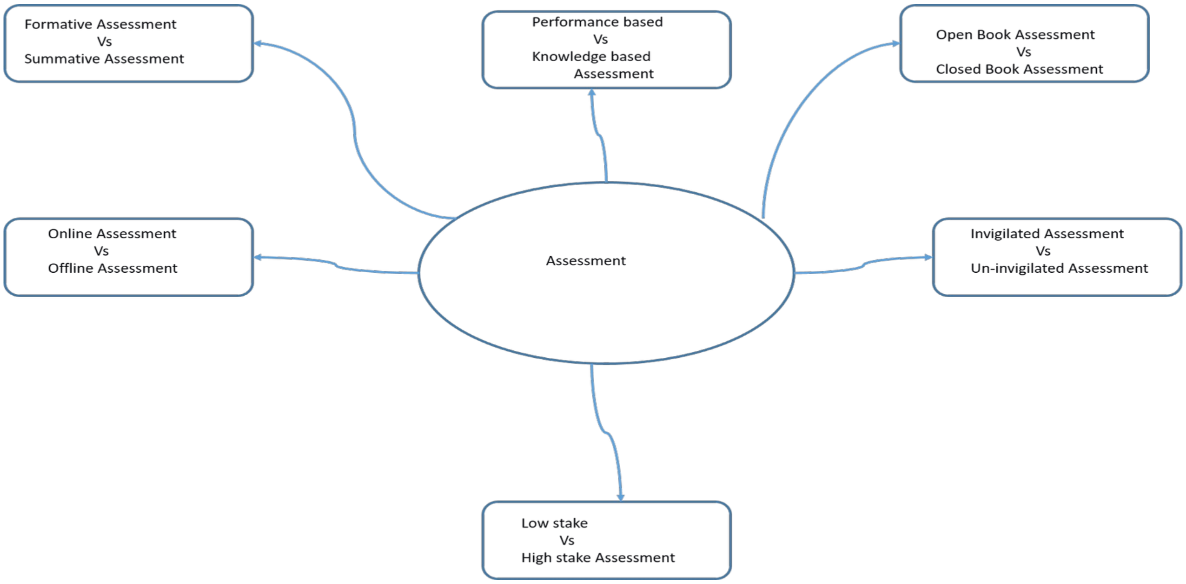


Figure 2.1: Types of assessment

Gupta (2017) defines an *"open book assessment"* as an assessment tool that is designed in such a way that it allows students to refer to class notes, summaries or “memory aids”, textbooks, or other approved material as they take the assessment. Gupta (2017) also uses the term “open book” in describing those assessments in which the questions are availed to students prior to sitting for the formal assessment and students have the latency to choose when they take the assessment within a specific time window and have the freedom to consult various sources as may be the case with a ‘take-home’ exam.

Based on Gupta (2017), *“closed book assessments”* are an alternative form of assessment whereby students should not refer to any material outside those tools or instruments that are prescribed by the assessor while carrying out the assessment. Further, Gupta (2017) justifies closed book assessments as a way of gauging how students can use the information acquired during the course of the study programme to solve problems or carry out certain tasks.

Van der Kleij, Vermeulen and Eggen (2015) and Black (2015) further reveal that the time when the assessments take place during the course of the study program and the contribution they make to the final course outcome can be a useful basis for classifying assessments. This alternative classification recognizes *“formative”* and *“summative”* assessments. Black (2015) defines *formative assessments* as assessments that happen during the course of study and aim to diagnose learning problems, encourage student learning and enhance performance.

Educators use formative assessments to consolidate the content covered as build-up to summative final assessments. Van der Kleij (2015) submits that formative assessments are useful in diagnosing the challenges that students may face in their learning efforts by providing feedback on student progress such as student strengths and misconceptions. In essence, formative assessments are *low-stake* assessments designed to identify needs and facilitate improvements; by contrasting the student's grasp of subject matter against the desired goal.

Formative assessments are *low-stake assessments*, that take various forms dictated by the content, the need and the situation. Gathuri et al. (2014) clarifies the common modes of delivering formative assessments as activities that are not assessable but provide feedback on progress. The authors describe formative assessments as tools for diagnosing and measuring issues or problems in teaching and learning activities or self-assessment quizzes that help students monitor their own progress.

Formative assessments facilitate the exchange of feedback from assignments, or from peers, colleagues, or mentors as the course progresses and promote dialogue and consultations with teachers, tutors, and other students (Black, 2015). They are typically used by educators and mentors to prepare students for formal and final examinations without contributing to the final grade.

According to Agboola and Hiatt (2017), *summative assessments* aim to report student achievement. In Higher Education, summative assessments are the *high-stake* assessments Fisher, McLeod and Savage (2016), describe summative assessments as inputs to key decisions such as promotion to the next class, certification, accountability, and completion. Agboola and Hiatt (2017) compares formative assessments against summative assessments and concludes that summative assessments demand more evidence of learning from the student and higher levels of reliability, accuracy, thoroughness, security and integrity from the assessment system.

Fisher, McLeod and Savage (2016) further emphasize that the value placed on summative assessments in Higher Education for qualification, certification and completion in particular, puts students under pressure to do their best as they hope to outperform their peers, appease their sponsors and families, earn qualification or promotion. Miguel, Ruiz and Blas (2018) discuss *performance or skills-based assessment* as a type of assessment which measures the ability of the student to perform practical procedures or tasks e.g. code a computer program, type text or perform a calculation. Skills-based assessments are practical by nature and contrast with *knowledge-based assessments.*

Miguel et al. (2018) generalizes knowledge-based assessments as those that are of a cognitive nature and place focus on the cognitive abilities of the student. Muukkonen, Lakkala and Toom (2017) present knowledge-based assessment as those that are taken in order to measure and prove the student's awareness of the body of knowledge applicable to a discipline. The researchers define knowledge-based assessment as formative and / or summative assessments that encourage the student to explore, tap, monitor, explain and discuss their own understanding of the subject matter in the discipline.

2.3.1 Conventional or physical assessment

The conventional or physical assessment environment can be described as a secured location such as a room that is specially set up to host the assessment event. The physical assessment is associated with conventional, face-to-face education in which the teacher and the student exist in the same "brick and mortar space" (Bohnsack & Margolina, 2019).

Kritzinger and von Solms (2006) describe the physical assessment venue as "a site deliberately quarantined to block out disturbances, provide a secluded and secure assessment setting."

Kritzinger and von Solms (2006) proceed and break down the setup of the environment into a set of three components i.e. staff that include educators, assessment managers and invigilators, students plus databases that carry the course and assessment data, assessment materials and grades.

The conventional paper-based form of assessment is the most commonly used form of assessment in contact or face-to-face education. Swart (2016) suggests that the conventional assessment system faces the challenge of high costs because it needs dedicated, specially equipped examination venues. Conventional assessment in such a physical facility therefore entails transportation costs for the students, institution staff, and the physical carriage of assessment materials to and from the venues. The assessment method also faces geographical

and scheduling challenges especially when the institution draws students from faraway places such as intercity, internationally or globally, as this has a bearing on assessment schedules.
Adil, Simon and Khatri (2019), Rodchua (2011) and Shon (2006) agree that measures implemented in conventional face-to-face assessments such as formal, recognized identity documents, or facial recognition by assessment officials as means to safeguard the assessment from impostors are "reasonably adequate" in the conventional assessment system. The authors reiterate that it is simpler to establish legitimacy in the 'conventional' face-to-face assessment environment than it is in other assessment environments because of the anonymity of the assessment taker, time and distance issues that characterize online education and assessment.

A recognized successful departure from conventional assessment is the case of University of South Africa (UNISA), Africa's largest open and distance learning institution. UNISA explored different assessment possibilities to cut down the cost, space and time challenges imposed by the conventional venue-based educational and assessment system to cater for its student base across the globe. The assessment options that UNISA adopted include take-home assessment and online assessments that students can take from designated venues across the globe. Swart (2016) reports that the results realized at UNISA are effective technology-enhanced assessments that can augment the conventional form of assessment.

2.3.2 Take-home assessments

Hall (2001) presents take-home assessments as those in which students receive test questions from the institution and tackle them away from the institution of study. The author explains that in Higher Education, take-home assessments are used to assess higher-order learning such as evaluation and creativity skills in which students are required to provide evidence of learning through essays, reports, assignments or participation in instructor-led discussions on electronic forums.

Hall (2001) positions take-home assessments as a prominent feature in the 'blended or flipped learning' approach to teaching and learning. The study also revealed that some Higher Education institutions incorporate Information Communication Technologies (ICTs) in take-home assessments and require students to submit their work on an online system or platform.

Weber, McBee and Krebs (2003) envisaged a blended pedagogy as ideal for the provision of a learning environment that encourages students to assume responsibility for their own learning. Relative to the other types of assessments, take-home assessments, Weber et al. (2003) associates blended learning with better student performance and speculates that better student performance in take-home assessments results from “the absence of invigilation, which reduces pressure on the student, as do the “softer” time limits characteristic of take-home assessments.” The authors hypothesize that the ability to take extra time to look up, cross-check and refine answers from various sources can increase students’ scores.

2.3.3 Offline assessment

Hervatis, Kyaw and Semwal (2016) define offline assessments as “… assessment processes that take place in the two distinct and discontinuous activities of performance and rating”. Tools such as questionnaires, assessment scripts, projects and assessment portfolios are used to collect evidence of learning from students.

A student performs tasks and submits some artefact for evaluation in a separate rating phase of the assessment process. Traditional pen and paper -based assessments that are typical in the physical assessment environment are qualified by Sarac and Karakelle (2017) as offline assessments.

Hervatis et al. (2016) clarifies the use of computer technology in gathering the evidence of learning or skill acquisition as an “offline” process if a time lag exists between the creation of the evidence and its submission for evaluation, arguing that the absence of a persistent electronic connection between the student’s computer and the assessment system renders the process “offline”. In this thesis, take-home assessments are thus regarded as “offline”.

2.3.4 Online assessment

James (2016) recognizes online assessments as:

“Assessment that is “in the presence of, and the facilitation of networks, the Internet, and related technologies”.

Watson and Sottile (2010) refined this definition to emphasize that in online assessments, the students attempt the assessment electronically through the course website. Bal and Fedeman (2011) present a detailed description of online education and assessment, focusing on the linkages that exist between the assessment, the student, the institution and the Internet. This detailed description is shown in Figure 2.2.

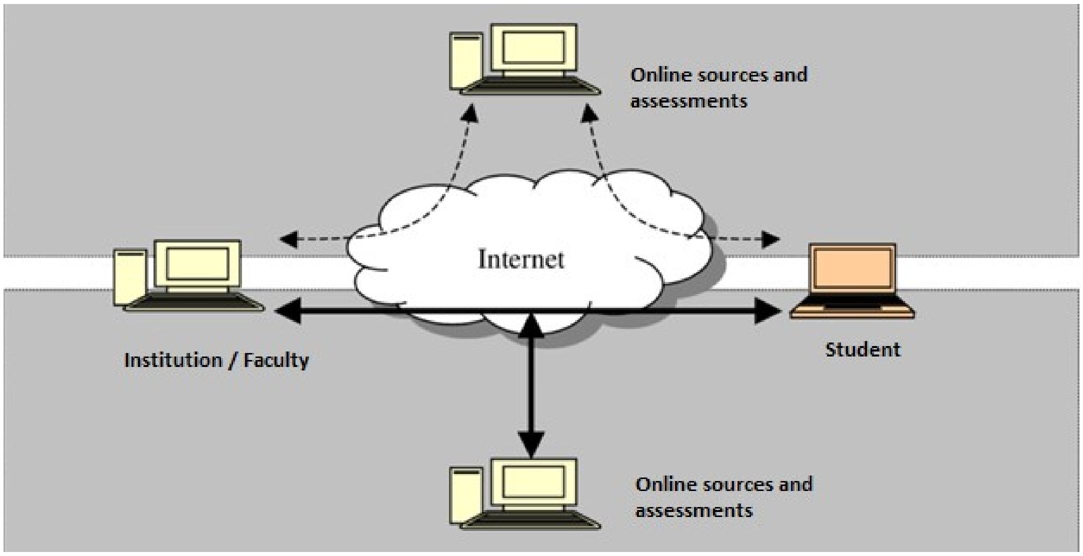

Online sources and assessments
Internet
Institution / Faculty
Student
Online sources and assessments

Figure 2.2: Online education

(Bal and Fedeman, 2011).

According to Hayford and Lang (2013), online assessments can take place in a central invigilated facility set up by the institution, in a manner similar to the conventional physical assessment, or students can take the assessment from any geographical location and at a time that is convenient to them. The authors elaborate that in the first case, examination systems and regulations similar to those used in conventional assessments can be adequate to secure the assessment.

Rowe (2004) argues that the high connectivity offered by modern technologies affords candidates learning off-campus the luxury of taking the assessment at any point in time and from any location. Rowe (2004) learnt that the online assessments provide a quicker and easier method for the evaluation of student progress and final assessment for a large population of students by defying or breaking the time and geographical constraints that characterize traditional assessments. Rowe (2004) concludes that assessing students online further reduces costs, compared to the traditional physical setting for both, the institution and the student because they discard travel, setup, and stationery or courier costs as they are paperless.

Wisher et al. (2005) agrees with the findings of Rowe (2004) but caution that the new modality of education presents the new challenge of ensuring that the student is identified “beyond doubt” as the genuine student who should partake in the educational activity.

James (2016) and Sun and Chen (2016) posited that credible online assessment is possible; provided the assessment and all the electronic connections involved are reliable and secure. According to Sun and Chen (2016), these challenges include the security of hardware devices that are brought in and connected to the institution’s server for use by the students in assessment. Such devices pose security risks as they are not owned or governed by the institution.

Mungai and Huang (2017), argue that implementing online assessments in a Higher Education environment avails numerous other benefits such as, automatic marking and grading, immediate provision of feedback to students, new opportunities for life-long learning and increased access for students living with disabilities or reside far from the institution. The existing online assessment systems fail to provide the time and space flexibility expected of online systems because most courses follow the conventional calendar of the traditional education systems. This requires students to take assessments at times and at locations designated by the institution (JISC, 2006).

Mellar et al. (2018) and Adetunji et al. (2018) show that many institutions are migrating assessments to online platforms. In these systems, a secure computer network delivers questions to the candidate, who provides the answers on an electronic device and submits them to a secure Learning Management System (LMS) for marking. Some LMSs immediately communicate the results upon completion. These assessments may be taken at a central assessment centre and at a set time or they may be decentralized and take place at a time selected by the student. For the centralized option, the institution must provide the infrastructure and personnel to invigilate the assessment. If the latter option is taken, then online invigilation software is required to secure and invigilate the assessment. Foster and Layman (2013) summarize the features of online invigilation of online assessments. Their findings are summarized in Table 2.1.

Table 2.1: A comparison of online invigilation products (Adapted from Foster & Layman, 2013)

Proctoring Features	Kryterion	Software Secure	ProctorU	B Virtual	Tegrity	ProctorCam	Loyalist	Respondus
Online proctor during exam	Yes	No	Yes	Yes	No	Yes	Yes	No
Continuous internet	Required	No	Required	Required	No	Required	Yes	No
Encryption for data transfer	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Schedule availability	20/7/362	24/7/365	20/7/362			15/5/?	24/7/365	
Proctor management	Yes	Yes	Yes	Yes	No	Yes	Yes	No
Supervised	Yes	Yes	Yes	Yes	No	Yes	Yes	No
Training	Yes	Yes	Yes	Yes	No	Yes	Yes	No
Career path	Yes				No	Yes	Yes	No
Certification	Yes		Yes	Yes	No		Yes	No
Interaction with test taker	Yes	No	Yes	Yes	No	Yes	Yes	No
Live chat	Yes	No	Yes	Yes	No	Yes	Yes	No
Canned messages	Yes	No			No	Yes	Yes	No
Live instruction to examinee	Yes	No	Yes	Yes	No		Yes	No
Proctor views examinee screen	No	No	Yes	Yes	No	Yes	Yes	No
Proctor as collusion threat	No	No	Yes	Yes	No	Yes	Yes	No
Prevent proctor view of screen	Yes		No	No	Yes	No	Yes	Yes
Later video review proctoring	No	Yes	No	No	Yes	No	No	Yes
Later video review capable	Yes	Yes	No		Yes	Yes	Yes	Yes
Control during test session	Yes	No	No	No	No	No	Yes	No
Test launch	Yes						Yes	
Pause test	Yes	No	No	No	No	No	Yes	No
Suspend test	Yes	No	No	No	No	No	Yes	No
Cancel test	Yes	No	No	No	No	No	Yes	No
Automated proctoring	Yes	No	No	No	No	No	No	No
Inappropriate keystroke	Yes	No	No	No	No	No	No	No
Audio levels	Yes	No	No	No	No	No	No	No
Real-time data forensics	Yes	No	No	No	No	No	No	No
Lockdown	Yes	Yes	No	No	Yes	No	Yes	Yes

Authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Webcam	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Logs/records	Yes	Yes	No			Yes	Yes	
Video storage	Yes	Yes	Yes			Yes	Yes	
Session review	Yes	Yes	No			Yes	Yes	
Time-stamped incident	Yes	No	No			No	Yes	
Incident logs	Yes	Yes (5 days)	No			No	Yes	
Program customization	Yes						Yes	
Levels of security decisions	Yes						Yes	
Allowed/specified aids	Yes						Yes	
Effectiveness research	Yes; Published	none	none	none	none	none	Yes; not published	none
Lockdown Features								
Owned or third party	Owned	Owned	None	None	Respondus	None	Owned	Owned
Windows and Mac	Both	Both	Neither	Neither	Both	Neither	Both	Both
Browser	Yes	Yes	No	No	Yes	No	Yes	Yes
Prevent browser control buttons	Yes		No	No	Yes	No	Yes	Yes
Prevent navigation	Yes	Yes	No	No	Yes	No	Yes	Yes
Prevent simultaneous tests	Yes		No	No		No	Yes	
Test exit controlled	Yes		No	No	Yes	No	Yes	Yes
Operating system/computer	Yes	Yes	No	No	Yes	No	Yes	Yes
Prevent right-click	Yes		No	No	Yes	No		Yes
Prevent printing	Yes	Yes	No	No	Yes	No	Yes	Yes
Prevent function keys	Yes		No	No	Yes	No		Yes
Prevent important key combos	Yes		No	No	Yes	No		Yes
Hide taskbar and desktop	Yes		No	No		No		
Hide menus and icons	Yes		No	No		No		
Prevent min/max windows	Yes		No	No	Yes	No		Yes

Prevent copy paste	Yes	Yes	No	No	Yes	No	Yes	Yes
Prevent running of applications	Yes	Yes	No	No	Yes	No	Yes	Yes
Prevent launch of applications	Yes	Yes	No	No	Yes	No	Yes	Yes
vent communication tools	Yes	Yes	No	No		No	Yes	
Detection support w/alerts	Yes	No	No	No	No	No		No
Inappropriate keystrokes	Yes	No	No	No	No	No		No
Response capture and use	No	No	No	No	No	No		No
Latency capture and use	Yes	No	No	No	No	No		No
Authentication Options								
Authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Username/password login	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Government-issued ID	Yes	No	Yes		Yes	Yes	Yes	
Photo comparison	Yes	Yes	No	No	No	No	Yes	No
Keystroke analytics	Yes	No	No	No	No	No	No	No
Challenge questions	Yes	No	Yes	No	No	No	No	No
Facial recognition	Yes	No	No	No	No	No	No	No
BioSig	No	No	No	No	No	No	No	No
Voice recognition	No	No	No	No	No	No	No	No
Fingerprint reader	No	Yes	No	No	No	No	No	No
Palm reader	No	No	No	No	No	No	No	No
Iris reader	No	No	No	No	No	No	No	No

2.4 Cheating in assessments

Diego (2017) qualifies cheating as follows:

“Any act that involves the possession, communication, or use of information, materials, notes, study aids or other devices that are not authorized by the instructor in an academic exercise.”

Hayford and Lang (2013) acknowledge as fact that students always take their chances and cheat in various ways through their educational assessments. Friedman et al. (2016) notes that in recent years, the phenomenon of academic dishonesty has gained momentum in Higher Education and the authors specifically mention the increase in dishonest behaviour that is enacted through electronic devices such as computers and personal cellular phones. Studies on academic cheating indicate that institutions have serious difficulties coping with all forms of academic dishonesty because they are concerned about the impact that it may have on their reputation and credibility. Consequently, many institutions tend to “sweep the issue under the carpet” (Brimble, 2016).

2.4.1 Cheating in physical assessment environments

This section looks into the ways in which students cheat in the “conventional” assessments, which characteristically take place under invigilation. Shon (2006) documented various ways by which students attempt to cheat in the physical assessment situation. His presentation included signalling systems designed by students to exchange answers with others even in the presence of invigilators, smuggling and sharing devices such as crib notes with answers in closed book assessments, copying, collusion and collaboration, the use of semiotics to communicate answers, the use of hi-tech gadgets and distracting the invigilator to camouflage such malpractices.

Physical education and assessment environments aim to give maximum security to the assessment hence in most situations, students have to produce some documentary evidence that they are who they claim to be (Sunday, 2014). Student authentication is thus ‘built into’ the mechanics of physical assessment as the student’s identity is validated before and during the assessment.

The physical assessment system provides security after the assessment as each artifact of the student's efforts is distinctly marked to identify the student. Kritzinger and von Solms (2006) reached the conclusion that face-to-face, invigilated assessments greatly reduce the likelihood of various forms of cheating such as collaboration and impersonation. Kritzinger and von Solms (2006) suggest that a level of trust and integrity is associated with the physical form of assessment; however, they also agree that impersonation still can take place. For instance, when a genuine student is substituted by a look-alike such as a twin.

Jenkins et al. (2011) established that facial expressions can affect the conclusiveness of facial identification and the student authentication mechanism using the face is not perfect because it hinges on the assumption that the invigilating official facially knows the students, that students produce acceptable identification documents such as National Identity cards, passport, driver's license and that the designated staff are alert, ethical and professional. Zheng et al. (2019) stresses that face-to-face assessments draw their high security rating largely from facial recognition as the invigilators usually know the student, check identity documents and stay in the presence of the student throughout the assessment.

2.4.2 Cheating in take-home assessment environments

Hall (2001) speculates that the take-home assessment gives students the privilege to take the assessment at a time and place of their choosing thus affording the student a more 'relaxed' atmosphere as they do not submit responses immediately, but during a prescribed "window period". Hovhannisyan (2018) acknowledges that take-home assessments present more opportunities for students to cheat especially through plagiarism. The researcher explains that plagiarism means that students copy content from external sources such as books, the internet, or copy from each other and claim it to be their individual work, not acknowledging the sources.

Dagilyte and Coe (2019) express the concern that by their very nature, the majority of students consider take-home assessments as open book assessments. The authors argue that this is not necessarily true, as educators do not always intend for the assessments to be open-book and that these yield students' submissions that are not an accurate reflection of their actual competencies or knowledge The authors expressed concern that not every student sees value in submitting their own work and that some students find it more important to submit work on time ahead of submitting their own work.

McCabe and Trevino (2001) posited that students cheat in take-home assessments through impersonation, in which case the student engages other parties such as paper mills or contractors and cheat websites to do the assessment for them. Paper mills and contractors provide and sell assessment related services such as writing full papers and theses under the names of paying clients. The fraudulent student obtains and submits answers from such sources or other knowledgeable third parties in a collaborative effort. Upon submission, the students claim ownership of the work.

2.4.3 Cheating in online assessment environments

In order to narrow focus and attention to academic offences committed online, Styron and Styron (2010), introduced the terms “electronic cheating” and “e-cheating” to describe various forms of student dishonesty or violations that employ information and communication technologies threatening academic integrity.

According to Sunday (2014), e-cheating exists in various forms, for example coded information stored on digital devices such as iPods and cellular phones may be smuggled into the examination venue. Students can cheat by downloading questions and answers from websites, or make use of mobile devices to exchange answers among candidates and other parties. Notes may be smuggled on digital devices e.g. pictures and voice notes into the examination venue. Some student may cheat by sending photographs of questions electronically to persons outside the examination venue and receiving answers via the digital device. In closed book assessments, students may cheat by browsing the internet for answers.

The challenge imposed by computer technologies on academic integrity is well documented in pedagogic literature. For example, Fask, Englander and Wang (2014), Blau and Eshet-Alkalai (2016), and Friedman et al. (2016) probe the relationship that exists between the extent to which technology is used as an enabling tool in assessments and the ease with which technology can be used to cheat in those assessments.

The inability of institutions to know with certainty the identity of the person taking an assessment, remains a serious concern in the community of academics and educational practitioners. Zviran and Erlich (2006) studied impersonation in an online environment and concluded that impersonation is difficult to detect or trap because the assessment happens from a place and at a time chosen by the student. Figure 2.2 is a basic illustration of an online education and assessment system, clarifying the spatial distribution of the elements that make up the system.

As explained in Section 2.2.3, the online education system characteristically has a distance separating the institution, student and assessment. Levy and Ramim (2007) explore the complexity of the challenge that exists in ascertaining the identity of the student and concluded that the challenge has led many institutions to adapting different measures to counteract the effects of impersonation. The study revealed that many institutions avoid the problem by hosting online and computer-based exams at secured physical centres where the problem of impersonation is reduced by using physical identification and invigilation.

Apampa (2010) points out that the challenges surrounding the credibility of assessments have become a big barrier in the establishment and recognition of online institutions and qualifications. To this day, academic practitioners continue to explore and discover ways in which students attempt to cheat in high-stake assessments.

Bedford, Greg and Clinton (2011) highlighted the need for accrediting institutions and government departments to make it a requirement for academic institutions that offer online programs, to prove the rigor and integrity of their online assessments, to levels that are similar to assessments conducted in physical, on-campus study programs and assessments. The authors challenge institutions in Higher Education to ascertain that the person registered for a program of study is the individual who does the academic work.

Some institutions employ computer-based technology to verify the persons taking assessments, against the enrolled student records. Bedford et al. (2011) concluded that such technology must extend to monitor the testing environment for the possibilities of other forms of cheating. Ramu and Arivoli (2013) emphasizes the need to preserve the security and academic standards throughout all the stages of assessment in order to build and retain trust and confidence in the assessment, as a true reflection of the student’s performance and evidence of learning.

Sarac and Karakelle (2017) explain that the” distance” characteristic of online and distance education opens room for academic offences such as impersonation, arguing that the distance between the student and the institution compromises the security and integrity of the assessment, potentially rendering the results of the assessment unreliable because there is little guarantee that the students took the assessment themselves.

Baleni (2015) noted that when students face challenges in online assessments, help from educators or the institution is not as immediately accessible compared with other forms of education and training. The author concludes that the apparent ‘deprivation’ of support, opens students up to various options and the possibility of cheating. Further research expanded the meaning of the term “e-cheating” originally introduced by Styron and Styron (2010) to include other malpractices. These expansions are summarized in Table 2.2.

Table 2.2: e-cheating research summary

Focus	Researchers
Accessing questions and answers in advance	Rowe (2004); Fisher, McLeod & Savage (2016)
Plagiarism of online works	Molten et al.(2013)
Online impersonation	Fisher, McLeod & Savage (2016)
Unfair retaking of online assessments	Rowe (2004); Friedman et al. (2016)
Unauthorized assistance from third parties	Akintunde & Selzing-Musa (2016), Onyema et al. (2019)
Collusion, contract cheating, engaging “paper mills” and subcontracted “ghost writers”	Moriati et al. (2016); QAA, (2016); Waghid & Davids (2019); Bretag et al. (2019), Onyema et al. (2019)

Contract cheating is defined as follows:

“A form of academic dishonesty where students get academic work completed on their behalf, which they then submit for academic credit or advantage as if they created it themselves” (QAA, 2016). Waghid and Davids (2019:22) clarify the term as follows “Ghost-writing or contract writing involves soliciting services of a secret writer and then presenting that writing as one’s own”.

2.5 The extent of cheating

Determining the exact extent of cheating in academic assessments has attracted a lot of attention and research efforts have yielded interesting findings. Roach (2001) argued that the sceptical view accorded online education and assessments, stems from the anonymity of the student in the eLearning system. Roach (2001) explained that the absence of face-to-face interaction lends the possibility that unscrupulous students can have others stand in for them during study and assessment. Roach (2001) further suggests that it is “impossible” to eliminate cheating in education. The author however, concluded with the hope that advances in technology will yield methods for preventing cheating in eLearning environments.

Pillsbury (2004) advanced the argument that the increased benefits emanating from the use of new technologies in education continue to be reduced by the growth of unethical behaviour among students. In agreement with Roach (2001), Adil et al. (2019) further argued that the prevalence and continuous advancements in technology made it simpler to cheat in assessments that involved technologies than in those conducted face-to-face or with pen and paper. Onyema et al. (2019: 3995 - 3996) believes that technology has improved the quality and integrity of examinations and can be used to mitigate examination malpractices. They caution however, that the emergence of some devices such as cellular phones and other portable devices have contributed to academic dishonesty.

Akintunde and Selzing-Musa (2016:111-112) and Onyema et al. (2019: 92-93) explored the reasons and motivations for students to cheat in assessments. These authors submitted a range of reasons why students cheat in their academic work. The major reasons submitted by these authors include the value attached to completion, low intellectual ability, fear of failure, anxiety, poor and inadequate preparation. Other reasons identified by these authors include the pressure from peers and families to excel, the laxity of the assessment systems in place, a lack of understanding the offenses, absence or “weak” penalties, poor supervision and moral decadence in the society.

The fact that some students cheat in assessments is established and some estimates of the prevalence of cheating on college campuses support this case Bolin (2004). Weber et al. (1983) argued that cheating was no more of a problem for take-home exams than it was for closed or open book tests in traditional settings, indicating that the environment or mode of assessment had no conclusive impact on the extent of cheating.

Rozycki (2006) indicates that most students somehow engage in cheating during their time in Higher Education. Patnaude (2008) studied the potential for cheating in online assessments. The study deduced that online assessments presented ‘relaxed monitoring’ of students giving the student the temptation and freedom to electronically share thoughts, ideas, and answers. In conclusion, Patnaude (2008) hinted that the lack of supervision in online assessments ‘justifies’ the perception that students are more likely to cheat in online assessments than in physical, invigilated assessments.

Sunday (2014) argues that with the advancements in information and communication technologies, and their increased accessibility, online assessment systems cannot keep with new and advanced means to beat even the most secure assessment systems. Deranek et al. (2015) countered Patnaude’s (2008) conclusions arguing that face-to-face Higher Education students subjected to traditional assessment methods were more likely to cheat compared to their online peers. Deranek et al. (2015) argued focusing mostly on the more stringent pressures exerted upon the student in physical environments such as strict dates, times and deadlines for completion of courseware and assessments as causes for more cheating in face-to-face than online environments.

Shaw (2004), Grijalva (2010), Hart and Morgan (2010) and Eckles (2010) concur on the point that online Higher Education students are less likely to cheat, compared to their counterparts in other assessment environments, as they suspect that their actions are traceable.

Diego (2017) revealed that 75% of students in Higher Education admit to cheating behaviour and 20% of the students in a study sample of 1369 admitted to having cheated in college.

Notwithstanding the debate on whether cheating is more prevalent in physical or online environments, cheating in its various forms does take place in assessments. With regards to impersonation, Rozycki (2006) concluded that impersonation posed the greatest concern and challenge to the very fabric that holds the academic community together.

2.6 Impersonation threat in online Higher Education assessments

In the past twenty years, research focusing on e-cheating shows a shift in research focus towards the implementation of new technologies that challenge academic impersonation. The Oxford Living Dictionary (2018: online) defines authentication as “the process or action of proving or showing something to be true, genuine, or valid”. In the context of computing, the dictionary qualifies authentication as the “process or action of verifying the identity of a user or process”.

Shyles (2002) and Rozycki (2006) revealed that impersonation in online assessments is a real challenge in academic institutions and one that researchers take seriously. In addition to these submissions, it appears that much research effort has gone into finding and refining ways to authenticate students, but less research into directly reducing impersonation. In this thesis, authentication means “verifying that the person partaking in the course or assessment is indeed the person who should be partaking” (Mahbub, Sarkar and Patel, 2016).

In online education, students engage in impersonation by having other people take studies or assessments in their place (Gathuri et al., 2014). This presents serious problems as individuals obtain qualifications, credits and recognition without acquiring the requisite knowledge and skills. Impersonation in online education obtains particular attention because of the absence of contact that is inherent in the system.

The nature of online education is such that the student is not ‘exactly known’ in the institution as is the case in conventional face-to-face education. Ullah (2012) focused on the inability of the institution to know all students closely, as a factor that makes good room for impersonation, where an impostor takes the student’s place. Other researchers such as Lee-Post and Hapke (2017), and Peytcheva-Forsyth and Aleksieva (2019) suggest solutions to the challenge of academic impersonation in Higher Education assessments. Table 2.3 shows some of the research projects that specifically target impersonation in online assessments.

Table 2.3 Research focused on academic impersonation

Researchers	Year	Research Submission
McMurtry, K.	2001	*E-cheating: Combating a 21st century challenge*
Levy, Y. & Ramin, MM	2007	*A theoretical approach for biometric authentication of eExams*
Moini, A. & Madni, AM	2009	*Leveraging biometrics for user authentication in online learning: A systems perspective*
McNabb, L	2010	*An update on student authentication: Implementation in context*
McAllister, C & Watkins, P	2012	*Increasing academic integrity in online classes by fostering the development of self-regulated learning skills*
Lee-Post, A & Hapke, H	2017	*Online learning integrity approaches: Current practices and future solutions*
Okada et al.	2019	*e-Authentication for online assessment: A mixed-method study.*
Peytcheva-Forsyth, R & Aleksieva, L	2019	*Students' authentication and authorship checking system as a factor affecting students' trust in online assessment*

The level of interest in academic impersonation justifies the notion that more research is necessary to find ways of minimizing impersonation in online assessments. According to Karim and Shukur (2016):

"…impersonation in online education is a deceptive action that targets to defraud the academic assessment system by standing in for a legitimate student".

The fraud implied in this definition from Karim and Shukur (2016) warrants interest and concern in reducing impersonation, as it has a bearing on the truth and credibility of assessment outcomes in society, industry, and business.

Impersonation in online education takes various forms including "paid impersonation", whereby an individual receives payment from a legitimate student to participate in an academic activity on their behalf (Shyles, 2002; Fisher, McLeod & Savage, 2016). Research has unearthed various methods that work towards detection, prevention, or combatting impersonation. Weippl (2005) points out that, unlike other cases of impersonation, in academic impersonation the supposedly "legal person" is not a victim, but an accessory to the fact and the act.

2.6.1 Types of academic impersonation

The ways in which impersonation takes place fall in four classes according to the mechanics of their conduct. Apampa (2010), Sabbah, Kotb and Saroit (2011) and Gathuri et al. (2014) all indicate that impersonation happens in various ways as presented in Table 2.4 (Apampa, 2010; Sabbah et al., 2011; Gathuri et al., 2014).

Table 2. 4: Impersonation threat types

Threat Type	Description
A	In an invigilated assessment, either the invigilator does not notice the case of impersonation OR they notice it and do not act against it for reasons such as bribery, coercion, or empathy. This is connived impersonation.
B	The legitimate student provides their security information to other parties who complete the assessment on their behalf purporting to be the holder of the identity given in the security information.
C	The legitimate student logs onto the assessment system and permits another third party to take the assessment on his or her behalf.
D	This happens when the legitimate student logs onto the assessment system and takes the assessment, working in a cohort with a third party.

Sabbah et al (2011) argues that threat Type A can only prevail in physically invigilated settings and considering the unrelenting advances in eLearning, the authors redefine the classifications shown in Table 2.4. Sabbah et al (2011) propose the following revised classification scheme to clarify how impersonation can take place in an online assessment environment. The reclassification is shown in Table 2.5 (Sabbah et al., 2011).

Table 2.5: Impersonation threat types (Sabbah et al., 2011)

Threat Type	Description
1	An impostor takes the online assessment for the student
2	The student takes the assessment but collaborates with a third party during the online assessment

With reference to Threat type 2, Sabbah et al. (2011) describes the complications associated with ascertaining the identity of the person who takes the online assessment because students take the assessments from different locations and at different times. Figure 2.3 illustrates the ideal or desirable online assessment system. In the ideal online assessment, the student who is registered by the institution is the individual who logs into the assessment and actually completes the course of study and assessment. The qualification and benefits are then attributed to the correct person.

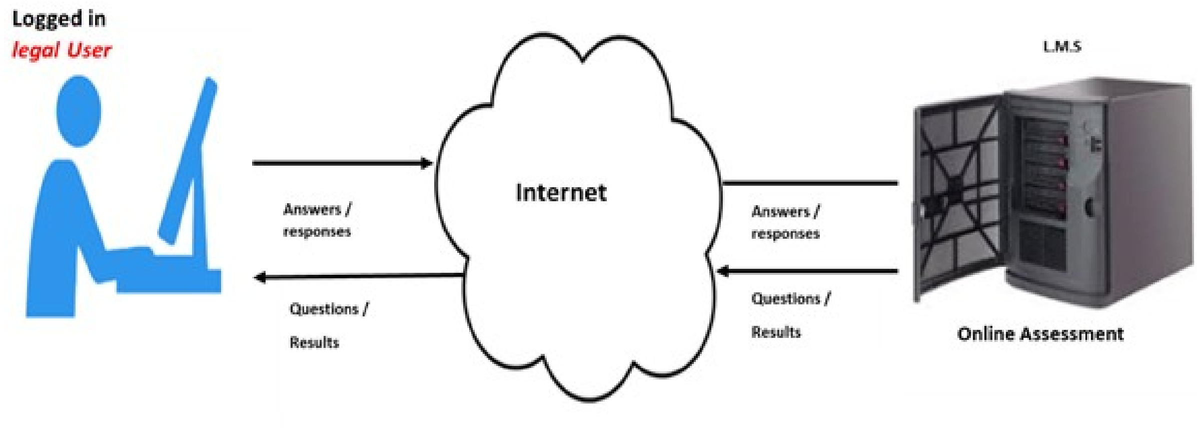


Figure 2.3: Ideal online assessment system
(Sabbah et al., 2011)

Figure 2.3A shows an example of impersonation Type 2 (Sabbah et al., 2011) or Type D (Apampa, 2010).

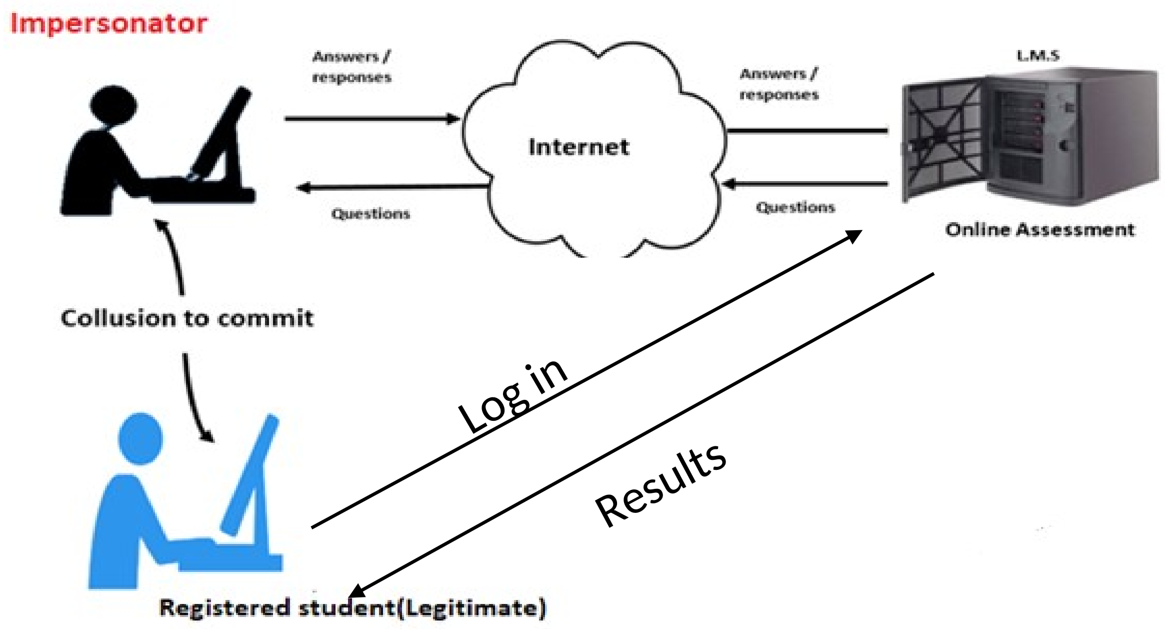


Figure 2.3A: Online assessment system with impersonation

(Apampa et al. (2010; Sabbah et al., 2011)

Stemming from these classifications, recent research (e.g. Okada, Whitelock and Holmes, 2019) has aimed at proving the presence, identity and authenticity of assessment takers. Some of the efforts that have been directed at maximizing authentication in computer-based systems are discussed in the next section.

2.7 Methods of fighting impersonation

The frequent challenges to academic integrity posed by impersonation on information and operational security in online Higher Education assessments gained attention from scholars. For example, Apampa (2010) sees an omnipresent need to ensure that the legitimate student accesses and takes assessments and must be confirmed to be the right student throughout the assessment.

Lee-Post and Hapke (2017 :137) summarizes that there are three possible approaches that institutions may engage to minimize online cheating: there is the “virtues approach”, the “prevention approach”, and the “enforcement” or “police” approach.

2.7.1 The virtues approach

This approach derives from the work of McMurtry (2001) and Bolin (2004) who argue that academic integrity can be achieved if educators take the necessary time to discuss the academic policy and the need for academic honesty in depth with their students. They suggest a precautionary approach and an educational perspective to cultivate good ethic and a level of honesty necessary for academic transparency. Olusola and Ajayi (2015:32) suggest moral intelligence as a way to inculcate fair practice and honesty in students as they define moral intelligence as “the capacity to apply moral principles in one’s own values, goals and actions (or the ability to see what is right and integrate it into one’s life and actions”

The virtues approach means that students are trained in self-discipline and discern the difference between right and wrong. The virtues approach seeks to develop students who do not want to cheat by increasing the students’ awareness to the disadvantages and risks associated with academic fraud. This can be achieved by educating students about academic integrity or dishonesty and institutional policy to clarify the terms and conditions, expected behaviour and practice. Olusola and Ajayi (2015) promote the idea of making each student attest to the policy ahead of engagement in studies or assessments.

2.7.2 Prevention approach

The methods found in this classification are manual or computerized strategies that aim to proactively block academic dishonesty from happening by eliminating or reducing opportunities for students to cheat. The methods also attempt to reduce the factors that pressure to cheat. Jones (2009) argued for a code of honour and pledge of authenticity statement that should be signed as a “rule of engagement” in assessments. This implies the need to educate students and foster in them an understanding of academic and institutional values of conduct and integrity. Jones (2009) further argues that the authenticity statement and code of honour provide a clear definition of academic integrity, its preservation, and the penalties of violation or non-compliance. The statement of authenticity must be signed as a declaration from students that the assessments they submit are genuinely their own.

McAllister and Watkins (2012) elaborate that in an online assessment setting, preventative measures can be implemented by periodically reminding students about academic policy content and implications. McAllister and Watkins (2012) recommended seven changes by which an online course can be re-modelled to incorporate students' self-regulation and discourage academic misconduct.

For the prevention approaches to be effective, an institution must promote a culture of academic integrity. This requires clear articulation of what constitutes academic integrity; faculty commitment to honour and enforce integrity practices and the deliberate development of integrity and self-regulation in students.

2.7.3 Enforcement / police approach

This approach is characteristically defensive and uses special strategies to catch and punish those who cheat. The focus in this approach is to detect and / or report academic misconduct and dishonesty after the fact. Heckler (2013) and Moten (2014) indicate that software intensive enforcements such as TurnItIn can be used to detect plagiarism in written assignments. Sewell et al. (2010) explored the use of Learning Management Systems (LMS) such as ColCampus, Blackboard, that use browser lock-down software such as Respondus to control a testing environment by preventing students from printing, copying, screen-sharing, screen-capturing, visiting other websites, or other applications while taking a test.

According to Hinman (2000), policing when employed consistently, can also serve as a preventative measure. The challenge to provide security in online assessment presents two real sub-challenges i.e. establishing and authenticating the identity of the student. Authentication can be used to confirm the identity, authenticity, and physical presence of a student engaging in online learning activities. Authentication technologies range from the basic user "User-ID and password" pair to biometric schemes and video monitoring.

Online student authentication aims to ensure that only registered students can access the Learning Management Systems (LMS) using some designated authenticators to identify and confirm the identity of the student. Studies by Rowe (2004) and Gathuri et al. (2014) conclude that security loopholes in online assessments arise from the fact that the assessments are taken at varied times and places. These researchers indicate that the authentication schemes used in online assessments generally perform identity verification at the commencement of the assessment and the majority do not continue to authenticate the assessment taker up to the completion of the assessment.

Heckler (2013) elucidates the dilemma and tension that exist between providing system friendliness or usability and providing adequate security in user applications at the same time. The authors highlight the need for effective post-login authentication as a requirement that must be met without disturbing the user's process or concentration with excessive authentication.

2.8 Methods of authenticating students or computer users online

Authentication methods attempt to reduce impersonation and academic fraud by verifying the identity given. Authentication technologies and methods are classified as knowledge-based authenticators, token / possession-based authenticators, biometric authenticators, predicative authenticators, environment authenticators, and human Invigilation.

2.8.1 Knowledge-based authentication (KBA)

KBA authentication methods use facts that are presumably known only by a legitimate person to determine the admissibility of the user to the systems services (Bowness, 2016). KBAs include the use of usernames and passwords or Personal Identification Numbers (PINs), as described by Ullah et al. (2012).

Zviran and Erlich (2006) rate knowledge-based authentication methods as the most common type of authentication systems. KBAs demand some secret security information which is presumably known only by the legitimate user. Based on Ullah et al. (2014), the common KBA methods include *username and password combinations and*, *challenge questions* that are drawn from the student's profile on the eLearning system.

Ullah et al., (2012) demonstrates that text-based questions, taken from academic, personal, favourite, contact and date domains could be effective for student authentication. The strength of the KBAs rests in their simplicity, low cost implementation and relative ease of use. According to Petra et al. (2016), a common challenge facing knowledge-based systems is that users may forget the information required, especially if it periodically changes, as is the case with passwords and Personal Identification Numbers (PINs). To avoid this, some users end up using simple passwords that are easy to guess such as dates or family names. Petra et al. (2016) propose using "cued-click" point graphical password. The authors argue that this scheme not only increases the password space, but also offers persuasive features and a means for users to capture their security credentials using images instead of text.

During registration or enrolment of the student, the authenticators to be used for the student are captured onto the system. These are kept in the system and updated as necessary. In assessment situations, KBA uses a dialog between the assessment system and the student in which the system poses questions and the student enters the answers, usually via a key device such as a keyboard. The technology is used extensively to log on to the assessment system after which a different authentication technology may take over. The process life cycle of KBAs such as usernames and passwords are summarized in Figure 2.4.

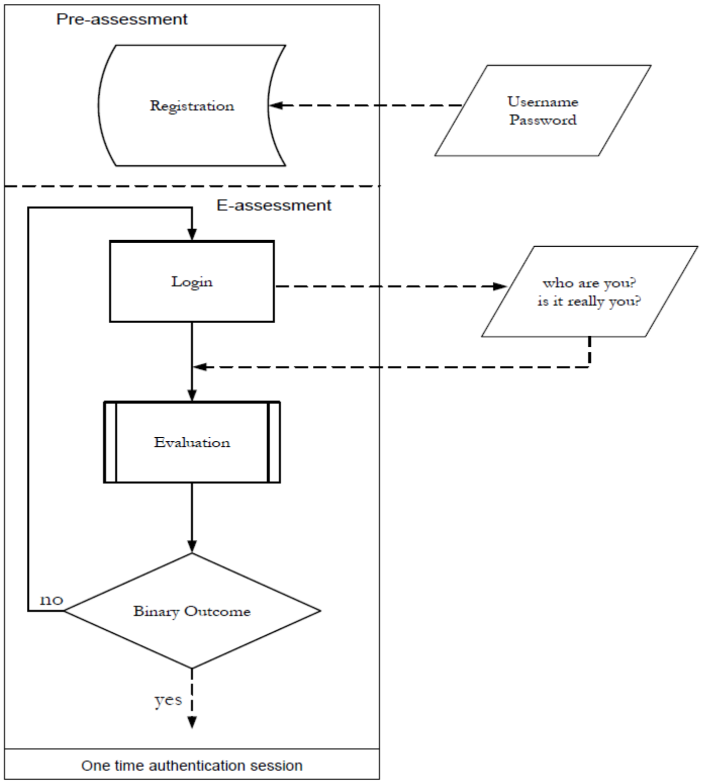


Figure 2.4: Knowledge-based authentication
(Ullah et al. (2012)

However, Ullah et al., (2012) argues that authentication based on the username and password or KBAs in general is inadequate to prove the identity and legitimacy of an online assessment taker. This inadequacy makes the assessments open to collusion and other attacks. The authors traced the weakness back to the sharing of the details that are subsequently abused in Types B, C and D impersonation generally and in Type A impersonation in invigilated online assessments.

Further, KBAs are only effective at the initiation of the assessment when the student initially logs in, but they are ineffective in light of the need for continual authentication of the student during the assessment. Xiao et al. (2009) and Fung (2017) agree that KBAs are weak because continuous authentication means the repeated provision of the username and password during the assessment which can be distractive for the student. This weakness reduces the effectiveness or usability of KBAs and limits them to the initial stages of online assessment sessions.

2.8.2 Token / possession-based authentication

These are methods that use an object assigned to the legitimate person for authentication purposes (Velasquez et al., 2018). Tokens can take various forms such as physical, in the form of Identity cards, digital devices such as pen drives and smart cards (Figure 2.5A) or soft tokens such as One-Time-Passwords (OTP). OTP authentication follows a process flow similar to the one described for password security in Figure 2.4. An OTP has a limited life span, typically 60 second time frames. When this time lapses and the user has not provided it to the system, a new unique value is calculated. Instead of sending an OTP to a registered user device, Agrawal, Paliwal and Sharma (2019) propose sending a scrambled image called a CAPTCHA image. When the user receives the image, they must decipher the image and capture it into the system for authentication. This method has become popular as a means of proving that the system is interacting with a human being and eliminates robots.

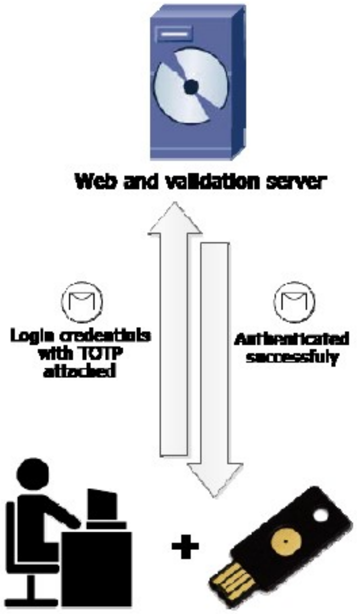

Web and validation server
Login credentials with TOTP attached
Authenticated successfuly

Figure 2.5A: Token based authentication
(Adapted from Marton & David, 2014)

Figure 2.5B shows an example of a CAPTCHA.

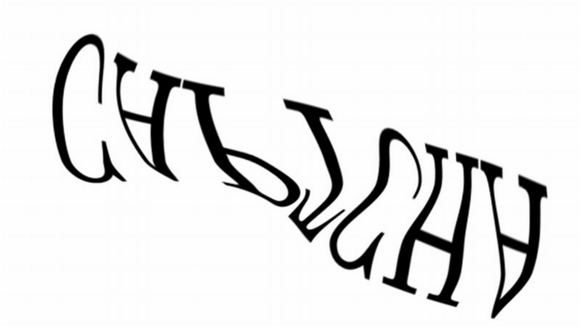


Figure 2.5B: CAPTCHA
(Adapted from Agrawal et al., 2019)

Ko and Cheng (2008) propose a token-based authentication scheme that uses encrypted student and assessment files stored on a zip disk. The authentication scheme uses a software mechanism to track the Network Interface Card (NIC) of the computer on which the assessment happens.

This proposal demands the registration or enrolment of a student's computer in a manner similar to KBA enrolment. The student would then be required to use the same computer for all academic transactions and interactions. Token-based authentication systems offer security only if the token is kept secure and safe from tampering through technologies such as encryption. Generally, as Weippl (2005) observed, students are complicit in academic impersonation. This means that tokens are not strong authenticators because they can be passed on to an accomplice in an impersonation scam.

2.8.3 Biometric authentication methods

Biometric authentication methods are relatively modern methods of authentication that use an indelible anatomical or behavioural characteristic of a person. Asha and Chellappan (2008) explain that the uniqueness of biometrics per individual makes biometric authentication superior when compared to KBAs and token-based authentication. Gao (2012) clarifies that biometric authentication frees the users of the need to remember passwords, patterns, and the need to carry tokens along with them because their being is the key to authentication. Biometric authentication uses real-time scanning of a user biometric characteristic and attempts to find a match with a previously stored encrypted data template.

Karim and Shukur (2015:170-171) discuss biometric authentication based on the Gaussian Probability Density function (GPD) which determines the similarity score between the stored reference template profile and incoming data (for which authentication is required). This GPD range is (0, 1) and the nearer the match is to one (1), the higher the probability that the incoming data subject is the same as the stored data subject.

In an online learning system, collecting the biometrics of the student happens during registration or enrolment through a biometric device that extracts or captures a biometric characteristic of the student such as fingerprint, voice or face. The biometric data is formatted and stored in a digital format as a template on a secure storage device (Bhagat & Katankar, 2014:975). The authors describe the process that happens when the system user logs into the system at a future time:

“The biometric device extracts the same feature from the student and submits the data to a matcher. The matcher retrieves biometric data from the stored template and searches for one that matches the incoming biometric reading.”

Karim and Shukur (2016) describes a match between the two values as the central condition for access to the application. Fung (2017) and Seo and Wyrwas (2019) hold the belief that the inception of biometrics presents much hope for a solution to the problem of authentication through effective and accurate methods of identification that cannot be shared or stolen. Biometric authentication is generalized in Figure 2.6 and Figure 2.6A.

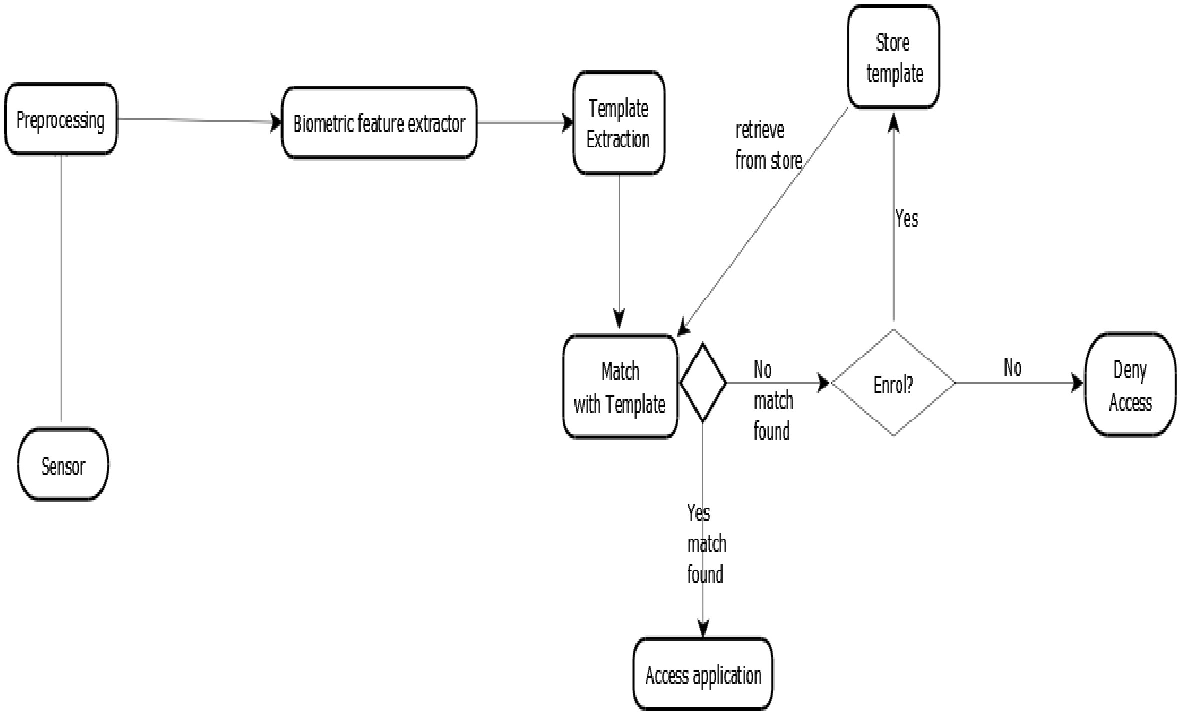


Figure 2.6: Biometric authentication
(Gao, 2012)

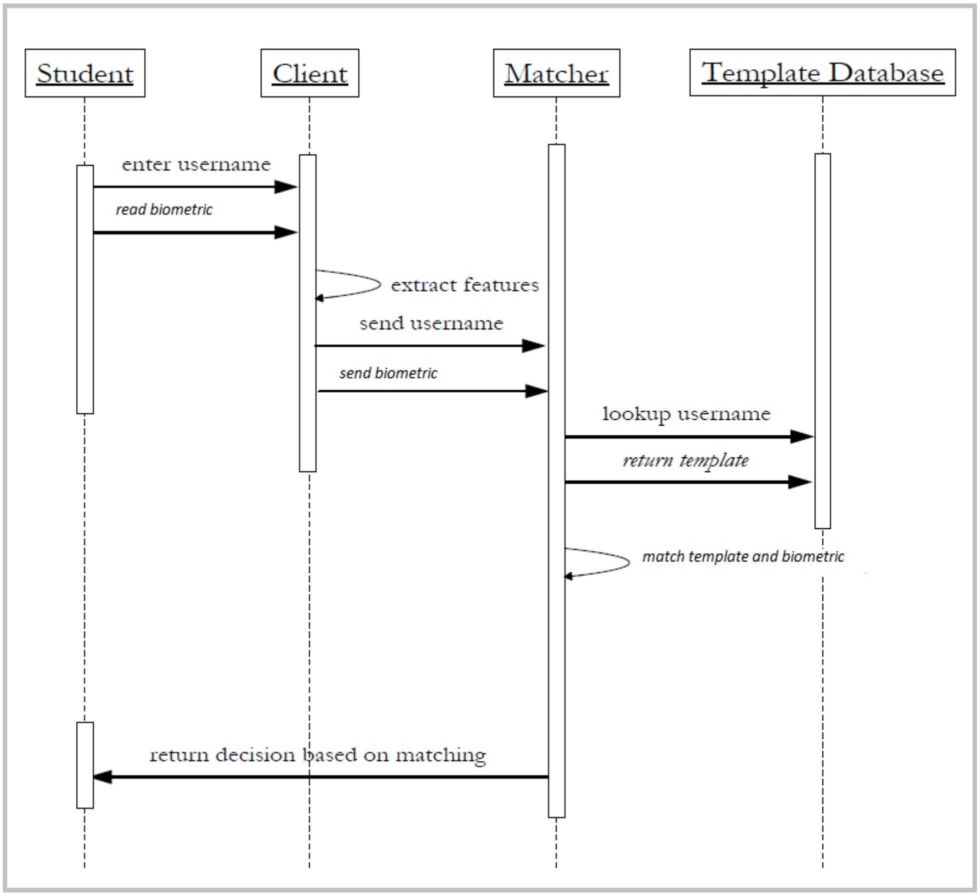


Figure 2.6A: Biometric authentication process
(Adapted from Apampa, 2010)

Rabuzin, Baca and Sajko (2006) explains that biometric authentication takes various forms. For example, the number of authenticators used in a system whether biometric controls are unimodal or multimodal. Unimodal biometrics utilize only one biometric feature of the user and the multimodal authenticators implement two or more features. Examples of biometric authentication technologies include fingerprint recognition, facial recognition, voice recognition, mouse movement dynamics, handwriting, iris or retina scanning.

2.8.3.1 Fingerprint recognition

Levy and Ramin (2007), Aggarwal et al. (2008), Alotabi (2010) discuss fingerprint biometric technology and agree that the technology is useable in eLearning assessments as they offer global uniqueness in the human race. The authors also agree that the usability of the fingerprint as a physiological biometric and a mono-modal authentication method faces challenges.

These challenges include the need for special scanning, hardware, the assurance of privacy and security of fingerprint templates, and storage problems as the volume of data grows. Seo and Wyrwas (2019) propose the advancement of on-screen fingerprint authentication technology for devices such as tablets and handheld devices as a worthy future direction for research and innovation e.g. the refinement of mouse devices that have a thumb print reader.

In online assessments, logging on using fingerprint scanning is of little value, in light of the possibility of impersonation when the legitimate student logs onto the system with their fingerprints detected and accepted but proceed to engage a different party to complete the assessment.

2.8.3.2 Facial recognition authentication

Panteado and Marana (2006), Agulla et al. (2008), Fayyoumi and Zarrad (2014), and Samangouei, Patel and Chellapa (2015) investigated the accuracy of facial recognition using images captured online through webcams and mobile cellular devices for matching with stored user images, applying pattern-matching algorithms. These authors all conclude that facial recognition could be useful for continuous authentication of online users.

The rationale behind the use of facial recognition for authentication is that facial recognition has a low demand for additional hardware, more so in the age of mobile computing which is characterized by the availability of high-resolution cameras on mobile devices such as notebooks. The problems associated with using facial recognition technology include the high processing power that it demands on the system. This factor limits the applicability of this technology (Samangouei et al., 2015; Andrejevic and Selwyn, 2019).

Further, Fayyoumi and Zarrad (2014) detail the challenges imposed by variables such as light, facial expression and capture angle, facial make-up, beard and spectacles, environment contrasts and weather conditions that make facial recognition highly sensitive. These issues reduce its usability and suitability as a single, mono-modal authentication tool.

Agulla et al. (2008) consider facial recognition in online systems as intrusive, distractive, and sensitive to ‘trivial’ issues such as beard, spectacles, angle of capture, head tilts and changes in posture that may lead to false readings.

2.8.3.3 Microphone-based and voice recognition authentication

Ramu and Arivoli (2013), Roberts and Page (2019) proposed using the voice biometric / behavioural trait in authentication methods in establishing the identity of the speaker and gathering information about the user's environment. Analysis of speech wave patterns both recognize the voice and put an identity on it. Rudrapal et al. (2012), proposed the use of voice recognition in continuous user authentication.

Hedaia, Shawish and Houssein (2020), submitted that users can be authenticated by voicing what they see is a CAPTCHA (Completely Automated Public Turing Test to tell Computers and Humans Apart). When the CAPTCHA is displayed to the user, the user pronounces the CAPTCHA for validation. The correct word must be said by the user and the voice must match the user's voice stored on the template.

According to Okada et al. (2019), individual variables such as voice pitch, speaking style, acoustic and accent qualify voice as a unique biometric trait. Factors such as varying speech speeds, noise and other external interferences, the quality of the voice capture equipment, limit the use of voice or speech recognition and reduce the robustness of the solution.

In online assessments, voice recognition cannot be an adequate measure against impersonation, as learners can theoretically be anywhere when they take assessments and they can take assessments at any time. The students have limited control over the environment in which they take the assessment. These points make audio-based authentication so environment-sensitive and a sub-optimal technique for the purpose of online student authentication Rao, Harshita and Dedeepya (2011).

In agreement with Rao et al. (2011), Okada et al. (2019) state that at its best, audio authentication through microphone input is useful as accompanying support for *other* methods to monitor assessment environments.

2.8.3.4 Mouse movement dynamics authentication

Ahmed et al. (2007) and Anima et al (2016), studied mouse dynamics to determine the uniqueness of each user's mouse behaviour. The way in which each user interacts with the computer using a mouse, creates a ‘signature’ that describes selected mouse movement characteristics. They argue that the resulting ‘signature’ is a product of complex application of statistics and Artificial Intelligence in the form of Artificial Neural Networks (ANN).

The possibility of using mouse dynamics for authentication was supported by other researchers such as Karim et al. (2017), and Li et al. (2018). Mouse dynamics such as movement, drag and drop, point and click and no mouse action are collected and stored on the database. As the user engages in a session with the system, for example during teaching and learning or assessment, the mouse dynamics are collected passively and analysed against the established profile for the user (Karim et al., 2017).

Almalki et al. (2019) submits that the mouse dynamics biometric is useable in eLearning, as it does not demand more hardware over and above the standard personal computer specifications. It is favourable because it provides continuous tracking and authentication of the user. Further, they jointly qualify the method as non-intrusive.

Li et al. (2018) and Almalki et al. (2019) conclude that on its own, the mouse movement biometric is weak when used in isolation, as it depends on screen resolution which informs user motions and must therefore be uniform between the biometric acquisition and the authentication processes, operating system settings, pointer speed and acceleration, which all impact user behaviour.

2.8.3.5 Keystroke biometric dynamics

Raul, Shankamarni and Joshi (2020) presents a statistical method, which uses time stamps for each key press and key release to establish the users’ ‘typing culture’. This method was refined by Araújo, Sucupira, Lizarraga, and Ling (2005) to include dynamics such as typing speed, pressure and the total time the user takes when typing a password and hit certain keys.

Araújo et al. (2005) details these measurements of performance on the way a user interacts with the computer through a keyboard and submitted the possibility of establishing the identity and presence of the user through typing ‘culture’ or habits. The keyboard typing profile is compacted and stored for reference when user authentication is required.

A number of researchers including Flior and Kowalski (2010), Saevanee, Clarke and Furnell (2015), Mungai and Huang (2017), and Raul et al. (2020) consider keystroke dynamics as a candidate's continuous authentication method for online assessment. The method is founded on the duration of each keypress and the time lag between successive keypresses which are collected as the input variables in building a user profile.

Keystroke authentication is useful in continuous authentication as it keeps track of the 'typing' pattern of the user throughout. It therefore detects and deters e-cheating through impersonation in keyboard intensive assessments.

The technology, however, has weaknesses and is unsuitable as a mono-modal authenticator. Mungai & Huang (2017), and Saevanee et al. (2015) concur that sampling the keystrokes to create an adequate profile for the user is complicated as shown by some weak results obtained in empirical studies.

2.8.3.6 Handwriting and signature systems of authentication

This method was suggested by Barclay and Yagolnitzer (2011) and refined by Hayashi and Akakura (2018) using tablet PCs, as a method to authenticate online users by providing a signature as a behavioural biometric when they initiate interaction with the assessment.

Handwriting based authentication requires the user to choose a digital signature pad, tablet, stylus, and mouse or touch pad as the input facility for drawing their signature Holden (2018). In user authentication, the system compares the drawn signature with a sample held on file. It is believable that the evident success of handwritten signature verification in commerce is sufficient to demonstrate its suitability for use as an authenticator in an online assessment environment.

Barclay and Yagolnitzer (2011) found that two basic schemes are employed in handwriting-based authentication; the first scheme uses static information held on file such as shape, width and density of the writing or lettering. Holden et al. (2018) elaborate the second scheme referred to by Barclay and Yagolnitzer (2011) and explain that the second scheme uses dynamic information such as the coordinates, writing speed, writing pressure and pen angle. Using signatures for authentication poses some challenges e.g. the need for extra hardware, software and the potential of forgery, are real challenges to the usefulness of the technology in eLearning systems.

Hayashi and Akakura (2018) argue that complicated algorithms, variations in signature on different occasions, caused by factors such as emotional and physical state, or physical setting, affect the quality or correctness of the signature. These factors reduce the capacity of signature or handwriting as authenticators in online assessment. At best, this technology is useful at the start or end of the session only, as it does not provide for non-intrusive continuous monitoring.

2.8.3.7 Palm print authentication

This authentication technology is based on the geometry of the user's palm. The palm print authentication technology's use in access control systems is common, but it has minimum usefulness in online environments as the input and security regulation only takes place in the early stages of interaction with the assessment system and discontinue once access is granted. Ullah, Xiao and Lilley (2012) point out that the technology needs special hardware and is not useful in continuous user authentication demanded in online assessments. Leng (2018) reported that palm print recognition can effectively be used in physical facility security and mobile devices. However, Jaswal, Kaul and Nath (2019) argue that palm print recognition is expensive and only effective as part of a multimodal authentication system.

2.8.3.8 Iris and retina scanning

These biometric authentication methods use features of the user's eye to determine and verify the legitimacy of the user. Bal and Acharya (2011) considered it as a very robust means of establishing identity in humans. The method is superior in establishing user legitimacy at log on. Zviran and Erlich (2006) recognize iris movement tracking can detect illegalities in the assessment environment. Gao (2012) cautioned that using this technology is expensive, owing to the grade of hardware required such as high-resolution cameras, storage demand from high volume data and privacy issues relating to retention on a database. Rabuzin et al. (2006) and Niinuma and Jain (2010), argued in favour of multimodal biometrics given that reliance on a single biometric feature was inadequate to meet the accuracy performance requirement of most applications.

2.8.4 Predicative methods of authentication

The past fifteen years have seen the addition to the body of authentication technologies methods that uses ‘predictive methods’ to prove the legitimacy of the user by establishing the user’s location or presence in front of the computer. Chuang et al. (2017) and Omolara et al. (2019) respectively, suggest and support the use of artificial intelligence to determine the computer user’s point of focus e.g. whether the user’s eyes are focused on the screen or away from it using iris and retina monitoring. This suggestion makes iris and retina scanning particularly interesting as a technology to detect the presence of other persons behind the user’s web camera.

As more scholars turn their attention to online assessment authentication, new technologies and devices continue to be explored, proposed and deployed. Lee-Post and Hapke (2017) propose a set of new, predicative methods of authentication. These include the ability to keep track of the physical location, the hardware used during the assessment, behavioural patterns and combinations of pre-existing methods, forming multimodal or multifactor authentication. The authentication measures in this category are efforts that do not qualify neatly in the categories described above such as authenticators that use Internet Protocol addresses (IP addresses) and Global Positioning Systems (GPS), timestamps, or video recording.

2.8.4.1 Environmental authenticators

Environmental authenticators work in two basic ways. Some attempt to establish the location of a user on the planet and use that to determine whether or not the source of a transaction matches the expected location (Mantoro et al., 2003). Another class of environmental authenticators attempt to authenticate user transactions by monitoring the environment in which the transaction takes place (Hamilton et al., 2017). Gao (2012) proposed a method of monitoring student activities using the Internet Protocol (IP) address of the device they use to take the assessment. The IP address points out the location of the device connected to the assessment system. Mahbub et al. (2016) describes the use of the Global Positioning System (GPS) to authenticate users of mobile devices using their geographical location.

IP and GPS tracking technology is useful on internet transactions, including online assessments, as it does not require additional hardware. This technology can provide a means of identifying suspect candidates who contract other parties at different localities to take the assessment on their behalf. This counter-measure is not perfect since an impostor can take the assessment using the device on which the legitimate student logged on (Type C threat according to Apampa et al. (2010).

2.8.4.2 Timestamps

Ko and Cheng (2008) define a Timestamp as a ‘mark’ that can be used to determine the date and time when an action or transaction transpired. Ismail et al. (2018) elaborated that although limited in its abilities to authenticating users, timestamping provides a basis for auditing. Ismail and Syed-Musa (2018) elaborate that when used together with an IP address, it gives a means of determining the device, location and timing of the interaction.

2.8.4.3 Video monitoring

Hernandez et al. (2008) classified video monitoring as an ‘affordable’ continuous user presence and authentication method that requires capturing hardware i.e. cameras and webcams. These devices today are easily accessible and come standard on most portable computers. Ullah et al. (2014) related video monitoring to deter and detect B, C, and D types of impersonation as described by Apampa (2010) and put forward its use in online examinations for remote invigilation.

Video monitoring faces challenges because of its intrusive nature, especially for candidates who take assessments in un-invigilated remote locations. Rao et al. (2011) observed that video monitoring might require either an ever-present and vigilant observer or storage space to store the footage. This means that the method requires the honesty of the student not to turn or shield the camera away from the desired angle of view and suggests that video monitoring needs augmentation with other tools to take good effect.

2.9 Using human Invigilation to secure online assessment

Abnave et al. (2017), described invigilation of online invigilated assessment system models after the traditional face-to-face assessment. This is where the students take the assessment in a predefined location and a pre-set date / time under the supervision of a human overseer.

2.9.1 Using face-to-face invigilation to secure online assessment

Rowe (2004) explains the operation of face-to-face assessment security as a system whereby students present some form of acceptable identification at the assessment centre, where each student is allotted computer equipment owned by the institution for use during the assessment. As a means of preventing cheating, the institution provides the hardware and ensures that the ports on the hardware that can facilitate external connectivity are disabled and the browsers set to allow access only to content deemed relevant for the assessment.

The method proposed here attempts to ensure that the assessment taker is legitimate. It is, however weak, in that it opens up the assessment to Type A threats (Table 2.4), and erodes the simplification, automation, accessibility and flexibility benefits of eLearning by restricting the place and times when the student can take the assessment. Jung and Yeom (2009) reflect on invigilated online assessments and report that invigilating online assessments leads to an increase in costs as travel to the venue and possible absence from places of employment. Jung and Yeom (2009) conclude that using this approach on final assessments and not on formative assessments may intimidate students. The authors argue that its use may be considered a lack of trust towards students. Furthermore, the authors pointed to the implied change in scene from the decentralized, remote learning to a centralized assessment environment as a factor that may reflect in diminished student performance.

2.9.2 Using technology for invigilation in online assessment

Online invigilated online assessment systems permit students to take assessments from any location, and involve a remotely stationed human invigilator (Sayad et al., 2014). This mode of invigilation is aided by different commercial products that are largely owned and run by third parties to provide rigorous student authentication (O'reilly & Creagh, 2016). The authors note that in some of the products, such as ProctorU™, the student engages in a chat with the remote invigilator, showing proof of identity, answering challenge or security questions (Ullah et al., 2014) and setting up the webcam for clear view. The student is also required to scan the room on camera to prove that they are alone and also keep the camera and microphone on throughout the assessment (O'reilly & Creagh, 2016).

The products offer different features and they have different focuses (Draaijer & Somers, 2017). For example, in some solutions, the remote invigilator may have the capacity to view the student's desktop, start/stop the assessment, talk to the student, and lock the browser. Other products can block screen printing, copying and pasting functions.

This means that students can open other websites including instant chat applications through which they can exchange content such as questions and answers during the assessment (O'reilly & Creagh, 2016). Such weaknesses mean that the student is not completely quarantined during the assessment session, making the assessment vulnerable to Type D impersonation (Apampa, 2010; Gathuri et al., 2014) through the possible involvement of other parties in the assessment.

Fenu, Marras and Boratto (2018) argue that human online invigilation is not scalable and suffers when the number of students is large, as the invigilator cannot practically pay full attention to each candidate in their care. The authors also point out the fact that third party invigilation service is expensive for the institution and student alike, as the service is billed hourly and therefore call for more research in the area of online invigilation products to compliment the rapid growth of online education, while controlling the overhead costs involved.

Hayton et al. (2018) argues against the use of third parties in the provision of invigilation services and suggests higher reliance on biometric control, artificial intelligence and less human involvement for online invigilation, to increase the reliability of authentication schemes and also preserve privacy.

Abnave et al. (2017) observe that the majority of existing technology-based invigilation solutions belonged in only one of the stated classes of identification and authentication i.e. unimodal and some relatively new solutions combined two or more authentication methods from different classes in an effort to reduce impersonation i.e. multimodal frameworks. In summary, Ramu and Arivoli (2013), Beaudin (2016) and Abnave et al. (2017) submit that some multimodal techniques take the form of frameworks.

2.10 Using frameworks for user authentication

The use of multimodal biometric authenticators attempts to raise the security of assessments and increases the likelihood of catching malpractice during assessments by combining two or more authentication schemes into a framework.

Figure 2.7 clarifies the multidimensional fight against impersonation as explained by Apampa (2010) which emphasizes using a method based on *Continuous User Authentication*.

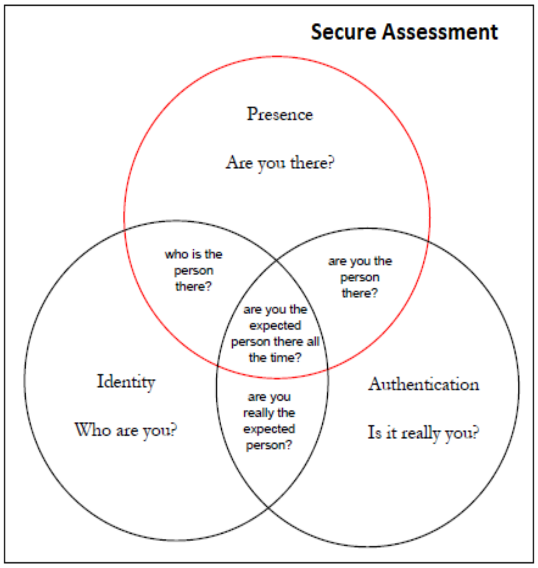


Figure 2.7: Secure Assessment Model

(Apampa (2010)

Apampa (2010) and Niinuma and Jain (2010) explored various techniques of ensuring that the correct person engages in the assessment using their Identity. The objective was to ensure that the person engaged in the transaction factually is who they claim to be. Through continuous authentication, cheating can be reduced by checking that the correct student remains in front of the computer throughout the period of the assessment. A three-dimensional model of continuous user authentication according to Apampa (2010) is shown in Figure 2.7.

This three-dimensional model gave much insight into the possible provision of user security against impersonation in online assessment. One implementation that uses KBAs running in tandem and creating a framework (Ullah et al., 2014) is shown in Figure 2.9. The framework proposes a combination of user login names and passwords with challenge questions derived from the student profile for authentication (Ullah et al., 2014).

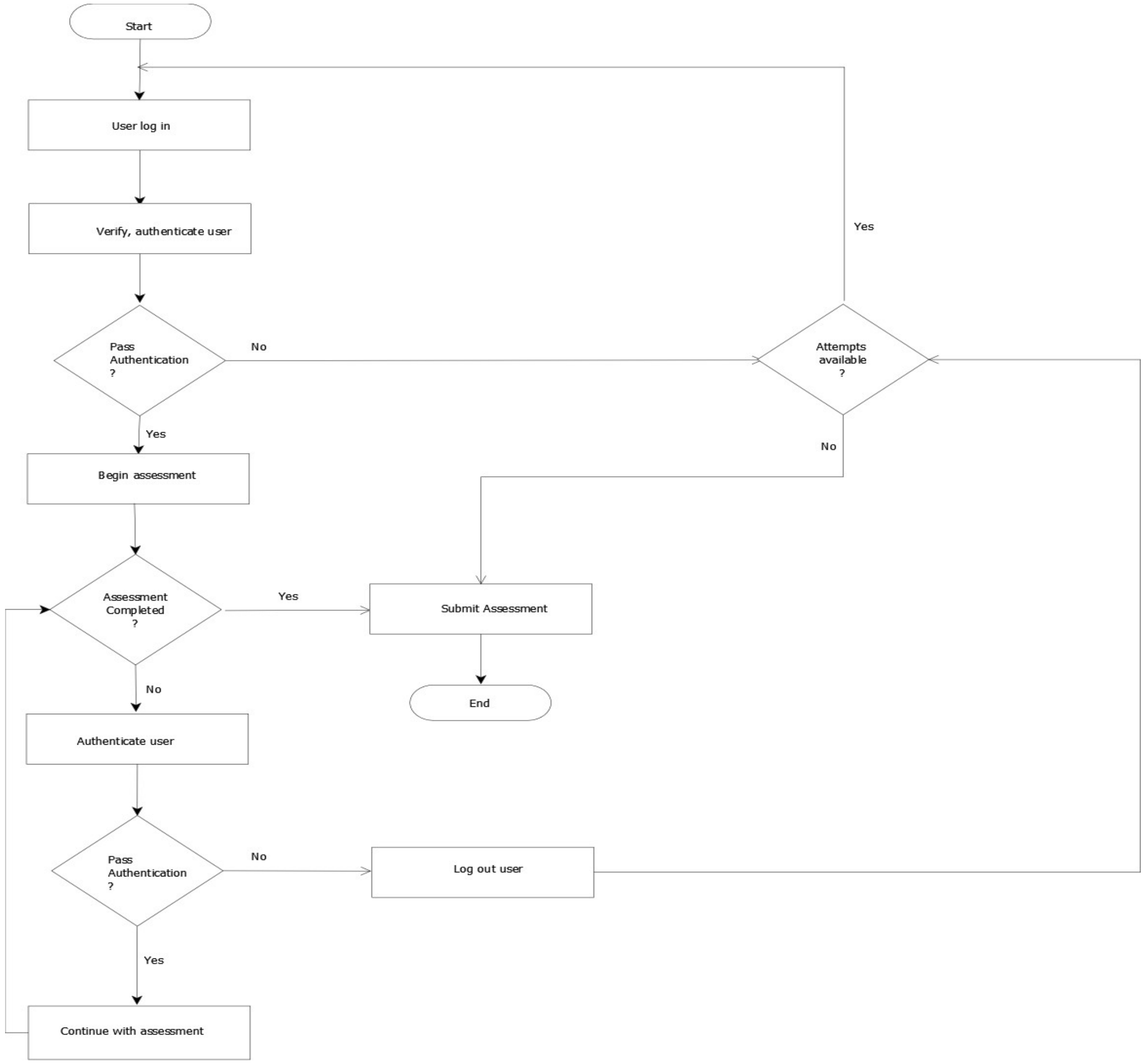


Figure 2.8: Continuous authentications
(Adapted from Niinuma et al. (2010)

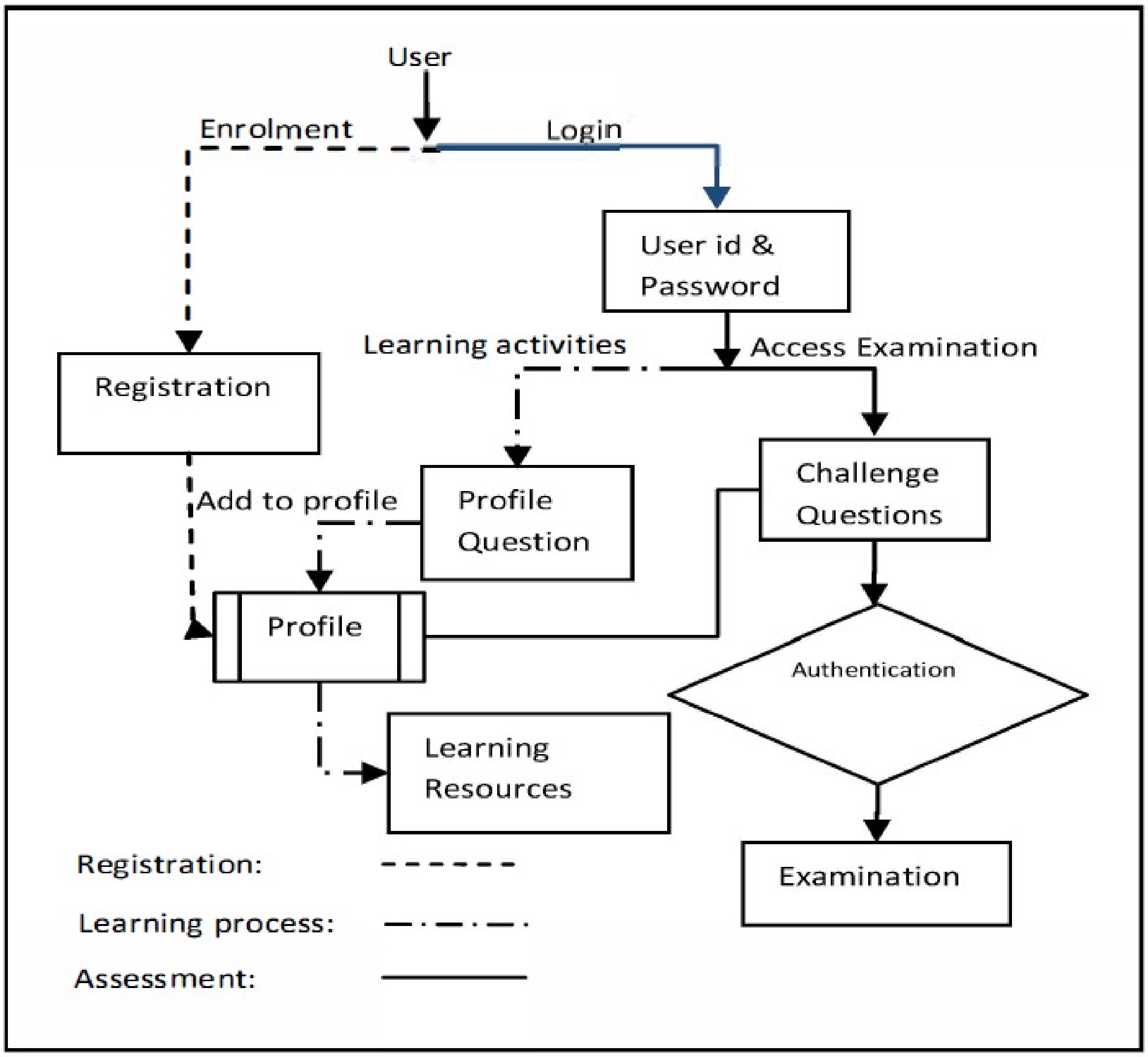


Figure 2.9: Authentication through challenge questions
(Ullah et al. (2014)

Ramu and Arivoli (2013) stressed the need for methods of authentication that guarantee the currency of the online assessments, ensuring the legitimate interaction between the student and the online examination, leading to authentic results. In their report, they informed that this assurance is based on having correct answers to the questions 'who are you?' and 'is it really you?'. These two questions point to identity and authentication, respectively. For online education, they derived a framework that applies to the authentication of users, regardless of the assessment modality (physical or virtual).

Saevanee et al. (2015) propose an authentication method utilizing linguistic analysis, keystroke dynamics and behavioural profiling, arguing that the framework could provide robust, continuous and transparent authentication (Ulinskas, Woźniak, & Damaševičius, 2017).

Okada et al. (2019) document a multimodal authentication framework known as the TESLA Project i.e. an adaptive trust-based e-assessment system for learning. This framework uses facial recognition, voice recognition and keystroke analysis to authenticate the student. The project also incorporates methods to combat other academic offences such as plagiarism through text matching and forensics.

For authentication, TESLA uses Student University Identities (SUDs) which incorporate static student email addresses, knowledge-based username and password, plus the biometric data as student IDs. The client-server architecture of the system uses three-tier exchanges to authenticate and secure data transfers.

The three-tiers are operationally independent and physically separate. When a student logs into the institutional Learning Management System, the SUD is channelled to the Virtual Learning Environment for algorithmic encoding. The output is a “blind signature” that in turn is channelled to the TESLA server for authentication before the assessment is launched and delivered to the student.

The result of the authentication server is channelled back to the VLE “blind” or encoded. The VLE performs the decoding and relays actual information to the institutional LMS. Figure 2.10 depicts the TESLA system.

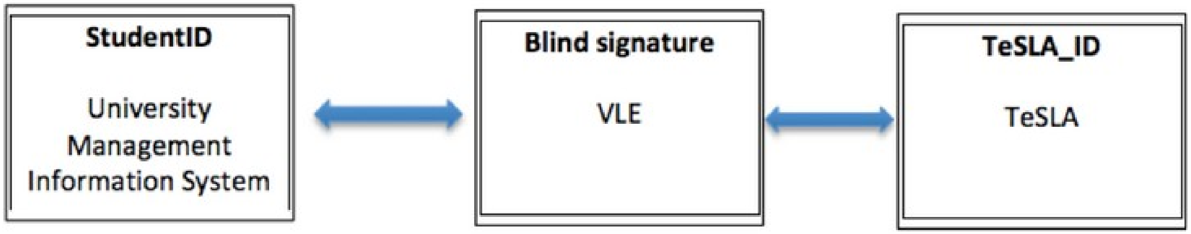


Figure 2.10: TESLA authentication
(Okada et al. (2019)

The literature review carried out for this thesis concluded that impersonation is a challenge in the online assessment that deserves further attention. More so, at Higher Education level where the stakes are high and not all assessments take place under invigilated conditions. More research is required to further the means by which less impersonation can prevail in Higher Education. One area that the researcher finds worthy of attention and bearing the potential to provide possible solutions is the field of Software Engineering.

2.11 Software Engineering (SE) as an approach to problem solving

The IEEE defines software engineering as an application of knowledge, principles, techniques and methods in a systematic, disciplined, quantifiable manner to the design, development, operation and maintenance of software (IEEE, 2014).

Kitchenham et al. (2011) describe the Systems Development Life Cycle (SDLC) as a systems engineering approach that provides a well-structured set of activities that result in the development of a performing software product. Figure 2.11 summarizes the activities that constitute the software development life cycle.

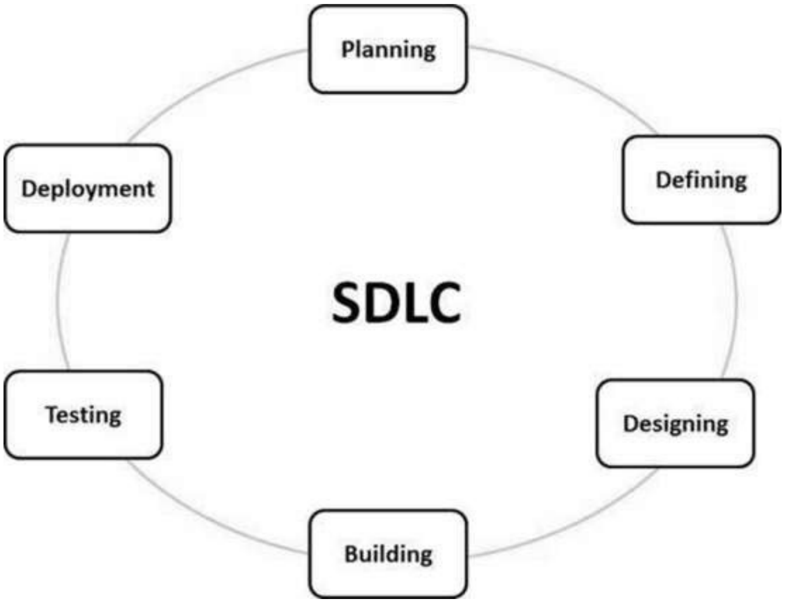


Figure 2.11: SDLC
(Kitchenham et al., 2010)

According to Kitchenham et al. (2010), the Systems Development Life Cycle comprises the following seven stages of planning, defining, designing, building, testing, deployment and maintenance.

2.11.1 Planning

The primary focus of the planning phase is gathering the core requirements from the stakeholders. The business systems analyst collects the requirements from the stakeholders and uses the information and knowledge acquired to formulate the Business Requirement Specification (BRS) for the software development planning, which also involves understanding the quality assurance requirements, the identification and resolution of the risks associated with the project.

2.11.2 Defining

When the BRS documentation is completed, a feasibility study is undertaken. The feasibility study is targeted at determining if the stated requirements are achievable in the contexts of the organization, available risks, available technology, budget, and opportunities. Technical feasibility gives a definition of the various technical approaches available for implementation of the project successfully with minimum risks. Organizational feasibility gives a picture of the suitability and applicability of the project to the organization, in line with its goals (organizational "fit"). Cost feasibility explores the favourability of the project in monetary terms and projects the monetary expenditures and benefits that relate to the project. The outcome is the Software Requirement Specification, (SRS), a document which contains a detailed explanation of the product requirements.

2.11.3 Designing

According to Kitchenham et al. (2010), the design phase is when the design specification in the SRS is created as a blueprint of the targeted software product. The design helps to specify the hardware and software architecture of the system.

2.11.4 Building

This phase primarily involves translating the design into an artefact such as a prototype of the software. The building stage brings the design blueprint into real life through the translation of the design logic into units of program code in a selected computer programming language. The instructions and logic are developed to spell out the exact steps that the computer must perform in order to realize its purpose (Mead, Garlan and Shaw, 2018).

2.11.5 Testing

Prior to the product being deployed, it is subjected to a series of tests to check for functionality, bugs, and run-time errors, against the requirements contained in the specification documents. Bugs or defects encountered in the test phase are reported to the development team for fixing. In an iterative fashion, the product is reverted to the test team for further testing. Kitchenham et al. (2010) describe this as an iterative process which continues until the application is stable and free from bugs and defects.

2.11.6 Deployment

Once the prototype or product is developed, tested and found to be completely in a working state i.e. in the context of the requirements, the product is installed or deployed in the working environment for use.

2.11.7 Maintenance

This is the operational phase when the targeted users begin applying the product and from time to time encounter some issues which they want developers to fix. The developer fixes the issues and software testers test the revised product before handing it back to the users.

2.12 Software Engineering

Software Engineering targets the production, implementation and management of software systems. Engineering methods are used to economically and effectively perform the processes through scientific and systematic approaches or technics.

Stage 1: Planning and Requirement Engineering (RE)

Requirement Engineering (RE) is the most important and fundamental stage in the Systems Development planning stage. Lemke (2018) isolates the primary focus of this activity as the collection of detailed expectations (requirements) of the software product's stakeholders from the problem domain. RE comprises of four basic activities i.e. Feasibility study, Requirements gathering, Software requirements specification (SRS) and Software requirements validation.

Stage 2: Defining Requirements

When the feasibility of the project is established, analysts and engineers engage users in a *requirements elicitation process* to find out details about what the software must provide and the features that they want incorporated. Requirements elicitation is the core of requirements engineering. Figure 2.12 presents a summary of the requirements elicitation process as Lee and Kotonya (2010) present it.

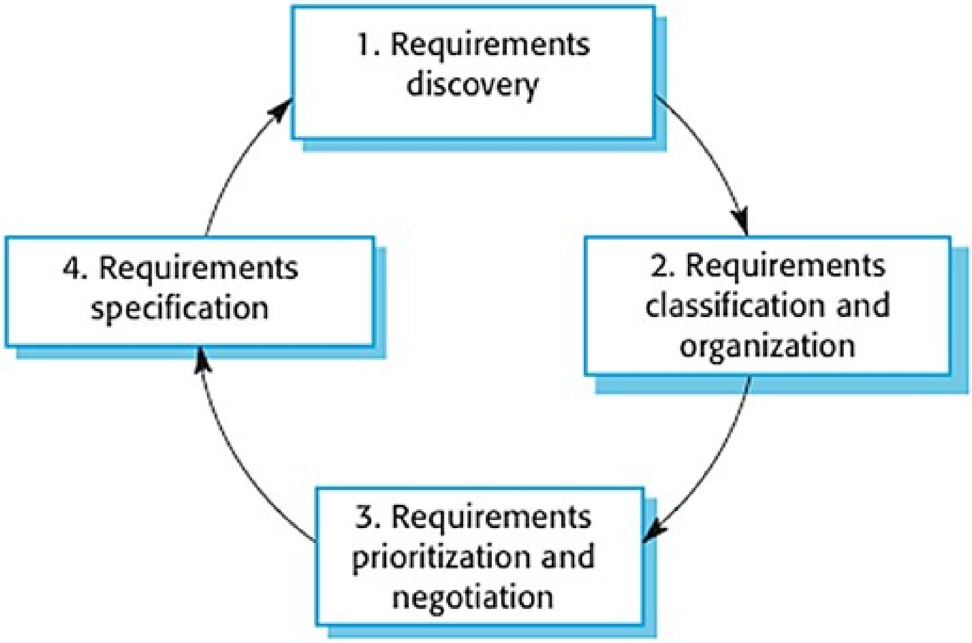

1. Requirements discovery
2. Requirements classification and organization
3. Requirements prioritization and negotiation
4. Requirements specification

Figure 2.12: Defining requirements
(Lee & Kotonya, 2010)

2.1 Requirements discovery

The development team discusses with the stakeholders to determine their needs and expectations. Requirements elicitation techniques commonly used include interviews, observation, document analysis, role-playing, prototyping, surveys, questionnaires, task analysis, domain analysis and brainstorming.

2.2 Requirements categorizing and organization

The information obtained using these tools in requirements gathering undergo analyses and categorization as user requirements, system requirements and functional requirements. Lee and Kotonya (2010) and Capilla, Jansen and Tang (2016), studied the importance, urgency and necessity of each requirement to the business as factors that form the basis to categorize and organize the requirements goals.

According to Laplante (2017), requirements fall in four categories. This classification of users' requirements in categories, serves a purpose in planning the basic project approach and in the feasibility study in the contexts of economic feasibility, operational feasibility and technical areas. Laplante (2017) presents the requirements as follows:

2.2.1 Must haves -The requirements in this category are central to the software product and the product will not be functional if it does not address the requirements that fall in this category.

2.2.2 Should haves - This category of requirements boosts the appeal of the software product and enhances the product in one way or another.

2.2.3 Could haves – This category carries requirements that are not central to the functionality of the software product but are peripheral to meeting user satisfaction.

2.2.4 Wish List – This category presents requirements that are outside the primary objectives of the software product, but stakeholders may desire them.

2.3 Negotiation and discussion

Requirements derived from the various stakeholders are studied in detail. Any ambiguities, conflicts, or duplications are discussed and negotiated with the stakeholders. Compromises, trade-offs and further categorization and prioritization are useful in refining the requirements.

2.4 Documentation

In the final stage of the requirements analysis, the Software Requirements Specification (SRS) formally documents the discovered requirements. The SRS is a document that clarifies the product requirements and serves as a vehicle of communicating the requirements.

The SRS contracts the development team to deliver the software product as defined therein. The SRS clarifies issues such as the *functional requirements, non-functional requirements, and user interface requirements.* The SRS also provides details of how the software will interact with the hardware and other external entities. Laplante (2017) demonstrated the need for software metrics and measures such as the expected response, resource consumption, quality, and limitations of the software to be included in the SRS to inform the rest of the development project.

Stage 3: Designing the software product architecture

Hilliard (2007) defines a software architecture as “the fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution”.

According to Bass, Clements and Kazman (2013), a software architecture (the target of this research) can be viewed as a high-level definition of a software system, which defines the components, the behaviour of the components and the interactions that take place between them. Software architectures are discussed in Section 2.13.

Stage 4: Building or developing the product

When the software design specifications get the approval of all the stakeholders, the actual development of the software product commences. The program code serving the specifications is created and software product testing runs in parallel with the development of each component or module.

Stage 5: Testing the product

Testing efforts characterize all the stages of modern SDLC models. However, this stage refers to the "testing only" stage of the completed software product where noted product defects are reported, tracked, corrected or fixed, and retested, until the product reaches the quality standards defined in the SRS.

Stage 6: Deployment in operations and maintenance

When the software product meets the requirements of the testing phase, the developers deploy or release it for use. Depending on the business strategy, the software product deployment may take place in piece-meal (phased in), by parallel run or in full (direct cutover). It is common for the product deployment to be initially limited to a segment for further testing in the real business environment.

This process is User Acceptance Testing (UAT). UAT provides the feedback needed to enhance the product for better performance in the targeted business operations. When released into operations, the software product is maintained to keep it useful to the user community.

2.13 Software architecture

Bass et al. (2013) define a software architecture as "an abstraction of the run-time elements of a software system during some phase of its operation. A system may be composed of many levels of abstraction and many phases of operation, each with its own software architecture."

Capilla et al. (2016), a software architecture justifies the need of architecture in software design, stressing that software architecture provides a bridge between the defined business goals, which are abstract, and the final concrete system. The authors explain that software architectures simplify the process needed to design, analyse, document and implement systems, using techniques that ensure the satisfaction of business goals and that software architectures solve business problems by defining the components of the software system, their boundaries, interfaces and interactions.

Software architectures can be considered tools that are useful in different ways to different stakeholders. For example, according to Hofmeister, Nord and Soni (1999), software architecture can be considered as a specification of the system to be implemented (blueprint) by software developers.

The architecture can be used as a tool or language for communication targeting a common understanding. From a management standpoint, an architecture can serve as justification for the choices or decisions about the system to be implemented and a documentation tool for current and future generations of users and developers. Mead et al. (2018) define the components that make up a software architecture as follows:

2.13.1 System Structures

According to Hasselbring (2018), system structures are the elements of a software architecture that abstract the composition of the architecture i.e. clarify “what the architecture is”. Hasselbring (2018) presents the elements of a software as follows:

2.13.1.1 Static / Modular structure

These define the computational capabilities and responsibilities of the software i.e. they qualify what the system will achieve. Examples of static structures are servers, libraries, databases and files.

2.13.1.2 Dynamic structure

The dynamic structure defines how the system performs its task when it performs the task, the synchronization of actions in response to stimuli.

2.13.1.3 Allocation structures

These describe the mappings between the static and dynamic structures to various environments including the organizational, developmental, installation and executing or operating environment. Figure 2.13 shows the general definition of a software architecture.

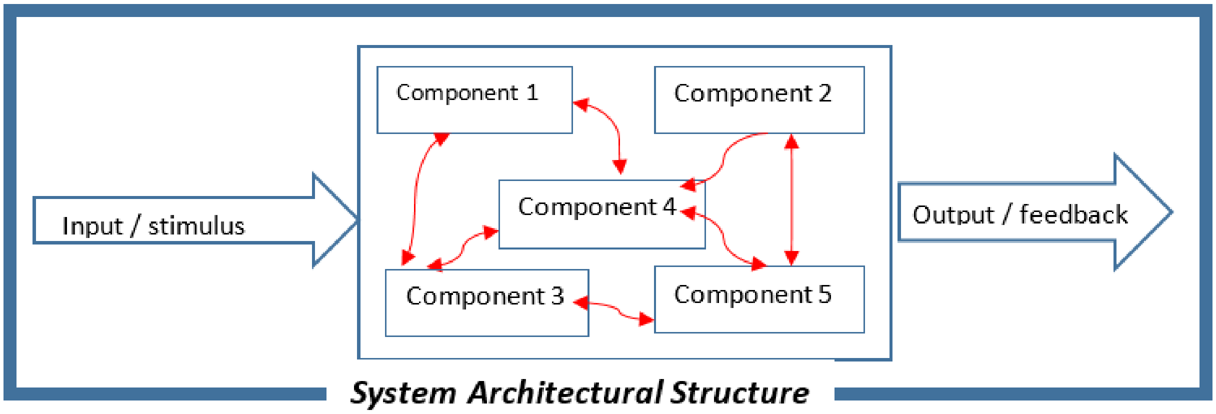


Figure 2.13: Software architecture

2.13.2 Externally visible properties

The externally visible properties of a system are the characteristics that define the system in terms of system operation and performance. These properties combine and give what the system does i.e. its operations in pursuit of its functional requirements. Externally visible qualities of the system performance complement the system structures by defining what job the software system does and how it does its job (Hasselbring, 2018). The externally visible properties pursue the non-functional requirements of the system Mead et al. (2018). Examples of the non-functional requirements of a system include speed, security, maintainability, adaptability and reliability.

Bass et al. (2010) recommended that a design approach should clearly define the architectural modules of the product and the associated data communication and data flow representation with external and any other third-party modules.
Definition and clarification of the static structure and externally visible properties of a software product is the core business of the Software Requirements Specification.

The SRS thus adequately provides the terms of reference for software product architects to determine the best architecture for the software to be developed (Hofmeister, Nord & Soni (1999). Based on the SRS, it is common that two or more software product architectures are proposed and documented in a Design Document Specification (DDS).

According to Bass et al. (2010), the DDS presents the software design in three basic forms:

2.13.2.1 Architectural design

The architectural design presents the highest level of the software product's abstraction. This design targets to give the software product designer an idea of the proposed solution.

2.13.2.2 High level design

The high-level design breaks down the architectural design into a more detailed, less abstract concept by giving a view of the subsystems, modules and the manner in which they interact with each other. This level of design details the static (modular and component) structure and the dynamic structure (interactions among components) at run time.

2.13.2.3 Detailed design

This design defines the structure of each module, its interfaces, communications and implementation. All stakeholders review the DDS to identify the best design approach for the software product. This process considers various parameters such as key functionalities, risk assessment, product robustness, design modularity, budget, documented performance metrics and constraints.

2.14 Chapter Summary

This chapter reviewed existing literature in academic assessment and discussed types of assessments used by institutions at Higher Education level. The challenges that student cheating in assessments present to academia; the causes and the ways in which students cheat were highlighted.

The Chapter drew attention to impersonation as a prime challenge in online assessments at Higher Education level. Chapter Two also summarized past and current efforts to fight impersonation in online assessments using Knowledge-based systems, Token based and Biometric systems. The literature reviews conclusively showed that impersonation is a challenge in the online assessment that deserves further attention. More so, at Higher Education level where the stakes are high and not all assessments take place under invigilated conditions. Current solutions generally present extra cost challenges or prove inadequate as they authenticate the student only in the initial stages of the assessment.

Authentication remains a challenge when students disclose identification data to others or conspire to have an impersonator take over the assessment after this initial identity and authentication phase. The findings of the literature review point to a need for more research into ways of fighting impersonation. This work aims to contribute by giving a software architecture that can improve online assessment systems.

Chapter three of this research presents details of a methodology to create a software architecture design for an online assessment system that discounts impersonation. The research is a design and creation project that uses the principles and practices of Software Engineering.

CHAPTER THREE
RESEARCH METHODOLOGY

3.1 Overview

The objective of this chapter is to describe the research design and methodology followed in this research project. The research design is a blueprint of the project and is designed to direct each step of the project. The design focuses on how the researcher executes the project to attain the objective laid down for the research. The research methodology specifies the procedures or techniques by which the researcher identifies, collects, analyses, interprets and reports information.

The theoretical foundations are necessary to support the research by providing concepts, the existing body of knowledge and provide a means of explaining and demonstrating how the findings of a research project support or dispel the existing theory (Denscombe, 2004). Each of these aspects must be discussed in detail.

Chapter Three presents the methods that the researcher selected for this software engineering project. The chapter is broken into the following subsections namely the theoretical underpinning of the study, research design, approaches to research, research strategy, sampling, data generation methods, transcription method, data analysis methods and techniques for evaluating the design.

3.2 Theoretical Underpinning of the study

This section gives insight into theories, principles and concepts that guided the researcher’s approach to solving the research problem that is detailed in Section 1.4. The concepts of Software Engineering that are summarized in Section 2.12 and Section 2.13 as part of the literature review are refined and explicated.

3.2.1 Software Engineering Design Theory and Principles

Further to the discussion in Section 2.11 of the literature review, Zhu (2005) submits that engineering and design must be based on scientific principles and technical information. The author continues to argue that the rationale underlying a design justifies the design by disciplined application and reference to such scientific and technological knowledge. This is to show how the targeted problem is solved, or why the design should be recognized as a solution.

According to Medvidovic and Taylor (2010), the nature of software engineering is such that one specific problem can be solved in innumerable ways i.e. the restricted problem space has an unrestricted solution space. The authors argue that "at the heart of every software system is its software architecture" and proceed to apply this design philosophy to software architectural development as shown in Figure 3.1.

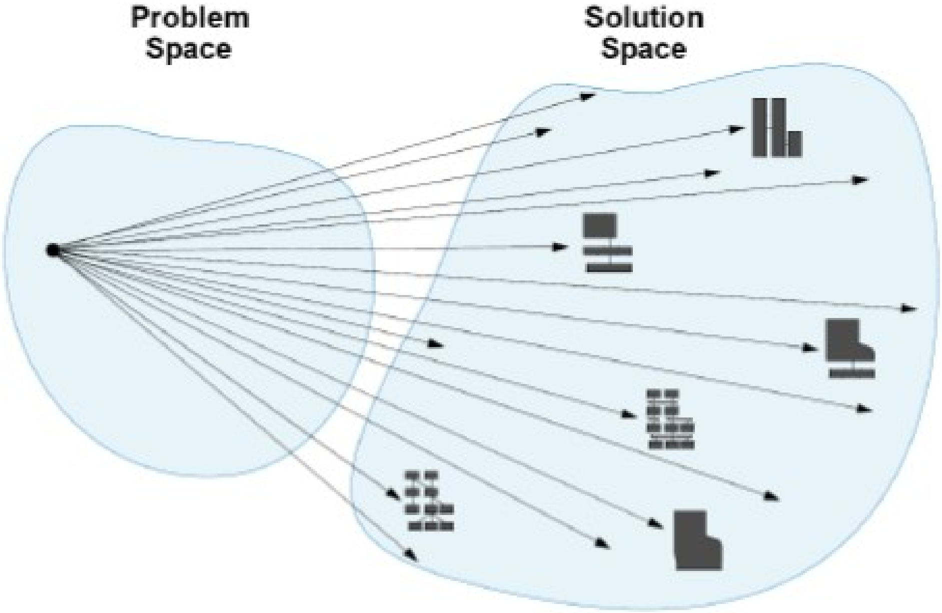


Figure 3.1: Problem space and Solution space in design
(Medvidovic and Taylor, 2010)

Figure 3.1 shows that for a single problem, a number of candidate alternatives can be identified and used as a basis for devising a solution to the problem.

Budgen (2003) presents a design process model that is applicable to software engineering and software architecture design (Figure 3.2). Budgen (2003) argues that the design must embody the production of multiple solutions and a subsequent process of objective comparison of solutions in context of presented requirements.

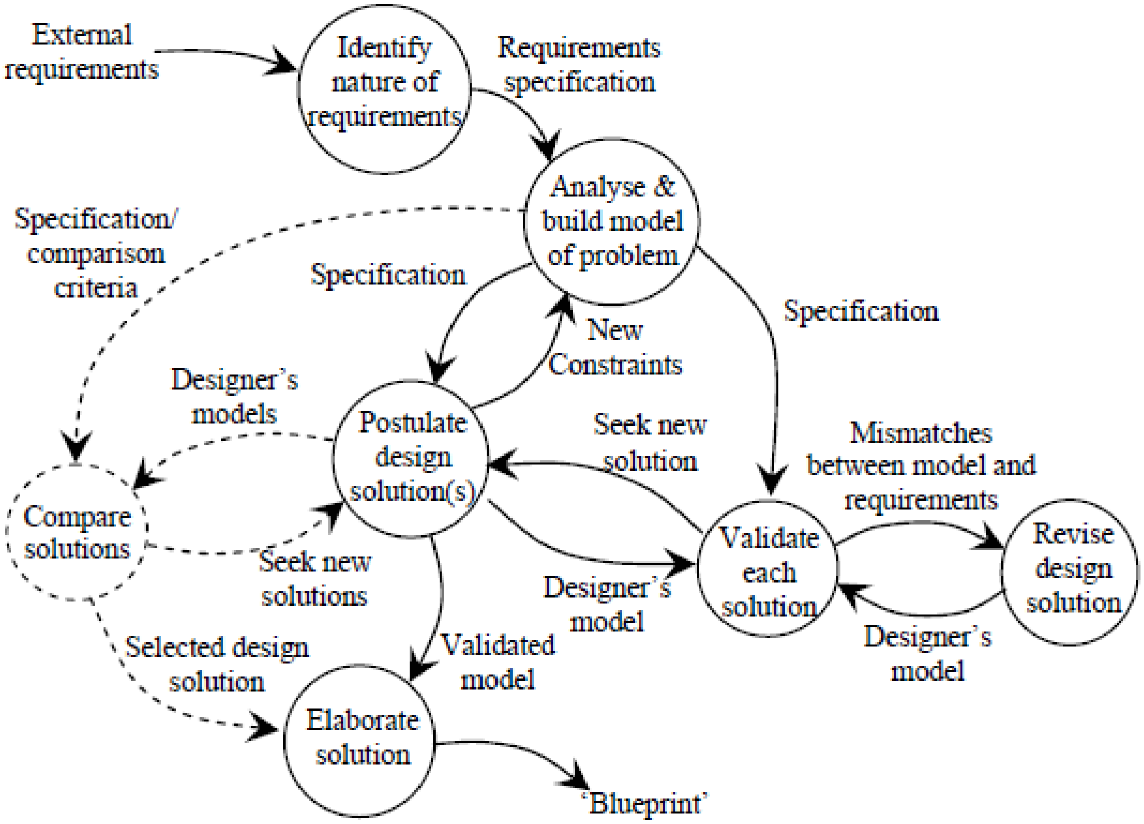


Figure 3.2: A general design process model

(Budgen, 2003)

This model is iterative in nature and can be summarized in a set of design activities. The activities are named solicit requirements, postulate a number of solutions, build a model for each solution. The subsequent activities involve evaluating the design against requirements (i.e. validation), comparing validated solutions and selecting one for further development, then elaborating the selected model to produce a detailed specification or blue print of the solution.

The strategies of design are typically iterative by nature and the exact method followed may be decomposition (Zhu, 2005), compositional, incremental / evolutional Cross (2003; Orlov & Vishnyakov, 2017).

Decomposition strategies take a top-down approach in design, systematically progressing from a high level, complex design to elaborate, simple design by strategically dividing the large problem into smaller and smaller sub-problems. The solution to the main problem is found by assembling solutions to the small sub-problems (Zhu, 2005).

Compositional strategies start by identifying a set of entities that are involved in the original problem. The entities are then described, classified and grouped. The relationships between the entities in each group are identified and links between the entities established. In the final design, the entities are progressively grouped to form the components of the model design (Zhu, 2005).

Incremental and evolutionary design strategies are described by Cross (2003) as “systematic trials and error approaches” which start with creating a design that only fulfils a selected set of critical requirements. On completing the design, it is evaluated against other requirements and necessary modifications effected on the design to incorporate the new requirements while preserving the features or properties that have already been satisfied.

Orlov and Vishnyakov (2017) posit a Criteria Importance Theory that may be applied in such evolutionary / incremental design to evaluate candidate designs and in selecting optimal solutions. The Criteria Importance Model (Orlov & Vishnyakov, 2017) uses criteria such as suitability, simplicity, scalability and interoperability to evaluate and rank alternative designs.

3.2.2 Software Architectural Design Theory and Principles

Perry and Wolf (1992) define software architecture using the following formula:

Software architecture = {Elements, Form, Rationale}

i.e. a software architecture as a set of elements, form and rationale. The following subsections summarize how the authors elaborate this definition of architecture.

3.2.2.1 Architectural elements

Data elements: The containers of data that characterizes the system, traverses or navigates the system and is transformed by the system.

Processing elements: These transform the data elements from one form or state to another.

Connecting elements: These elements act as the “adhesive” holding together the different pieces of architecture. Examples of connecting elements are procedure calls, access to shared data and messages exchanged between components at run time.

3.2.2.2 Architectural Form

Architectural form comprises weighted system properties and relationships (Perry and Wolf, 1992).

Relationships constrain the positioning and organization of architectural elements in the system i.e. their placement and interaction within the system.

Properties are constraints imposed on the choice and behaviour of architectural elements in a system.

According to Perry and Wolf (1992), properties and relationships define the minimum expected or desired features, properties or behaviour of architectural design. The expectations imposed on the system are regulated using weights or indicators of the importance of each property or relationship. The weights are used in ranking preferences and in taking choices when faced with competing alternatives.

3.2.2.3 Architectural Rationale

The rationale for taking various design choices in the definition of an architecture serves as motivation for specific combinations of elements, form or architectural style.

In the final analysis, Perry and Wolfe (1992) define software architecture as a document that prescribes how a system is to be built and operates. In summary, the authors argue that “architecture is concerned with the selection of architectural elements, their interactions, the constraints on these elements necessary to provide a framework in which to satisfy the requirements, serving as a basis for design”.

Gacek et al. (1995) take up this prescriptive definition (Perry & Wolf, 1992) and add that a software architecture system must contain statements of stakeholder requirements. Gacek et al. (1995) argue that satisfying stakeholder requirements is central in architectural design and development.

Shaw and Garlan (1996) treats software architecture from a descriptive point of view by focusing on describing architecture as a high level structure in terms of architectural elements and interactions amongst them. In their submission, Shaw and Garlan (1996) state that “abstractly, software architecture involves the description of elements from which systems are built, interactions among those elements, and the patterns that guide their composition and constraints on those patterns."

Shaw and Garlan (1996) concur with Gacek et al. (1995) in emphasizing that there must be correspondence between the system requirements derived from stakeholders and the elements of the constructed system. In contrast with the prescriptive definition of Perry and Wolf (1992), the authors identify only two parts as the basis of architectural design. The parts identified by Shaw and Garlan (1996) are:

Components: A component is a unit of software that achieves a defined function at run time e.g. software programs, objects, processes, servers, clients and databases.

Connectors: A connector is a mechanism that mediates between components enabling communication and synergy between components. According to Shaw and Garlan (1996) implementation and realization of requirements are often distributed across the system and jointly achieved by many participating components at run-time e.g. accessing shared values, procedure calls, message passing protocols, data streams and transactions.

Essentially, Shaw and Garlan (1996) highlight that software architectures can exist in a hierarchy whereby one system may be composed of many, smaller systems; each of which may have its own architecture. The authors draw attention to abstraction, by which the specifics of how the components and connectors at each level are implemented remain hidden in the architectural definition, enabling differential implementation.

Perry and Wolf (1992) present a prescriptive view to software architecture and Shaw and Garlan (1995), in contrast, provide a descriptive view. Bass, Clements and Kazman (2013) define and view software architecture in the context of multiple views. Hasselbring (2018) argues that owing to its complexity and invisibility, the structure of a software-based system can be viewed from different perspectives. This results in a number of different models of the same system, each of which is limited and pays attention to only a specific set of properties, components, features or functionality of the system and abstracts the rest of the system. This explains why the authors define software architecture in terms of abstracted components and externally visible properties, each viewed as sufficient only for some clear purpose or audience.

Bass, Clements and Kazman (2013) present software architecture as "an abstract representation, or model, of a complicated system defined in terms of its structure, consists of a collection of components together with some relation among them to achieve certain engineered purposes and to manifest a certain set of properties of interest on the system”.

In a subtle way, the authors suggest that software architecture comprises components, externally visible properties and structures.

Components: To emphasize the expected level of abstraction, Bass, Clements and Kazman (2013) deliberately avoid clearly defining “component’ arguing that architecture can comprise more than one kind of component, more than one kind of structure, and multiple modes and types of interaction among them (Hasselbring, 2018),

Externally visible properties: According to Bass, Clements and Kazman (2013), these are the assumptions that “components” can make over other “components” e.g. the services it delivers, performance characteristics, and shared resource usage. The authors use this definition to abstract information from the system and yet provide enough information for function delivery and efficient interaction.

Structures: Hasselbring (2018) characterize a system in terms of its components (units), and their interactions (links). Each structure is associated with its uses in the software system development. Examples of structures as defined by Bass, Clements and Kazman (2013) include logical or context structure, module structure, process structure, control flow structure and class structure.

In this thesis, the definition of software architecture combines concepts and principles from the prescriptive view (Perry and Wolf, 1992; Gacek et al. (1995), the descriptive Shaw et al. (1995) and the contemporary work of Bass, Clements and Kazman (2013) and Hasselbring (2018).

3.2.3 Building a software architecture

According to Nuseibeh (2001), the development of requirements and software system architecture must happen concurrently in order to increase productivity and stakeholder satisfaction. The author argues for an early understanding of stakeholder requirements and the construction of a software system architecture that provides for the discovery of further or more refined requirements and constraints, technical feasibility, and objective evaluation of competing designs.

The “Twin Peaks” model (Nuseibeh, 2001) presents a development model characterized by concurrent, iterative, processes that deliver increasingly detailed requirements and design specifications i.e. as the requirements become clearer, so does the software system architecture. The author argues that such development is useful as it can withstand rapid change and emerging requirements. Essentially, the “Twin Peaks” model accommodates realization of new requirements by allowing early exploration of the solution space, facilitating stakeholder interaction in design and incremental (modular) development and risk management. The “Twin Peaks” model is shown in Figure 3.3.

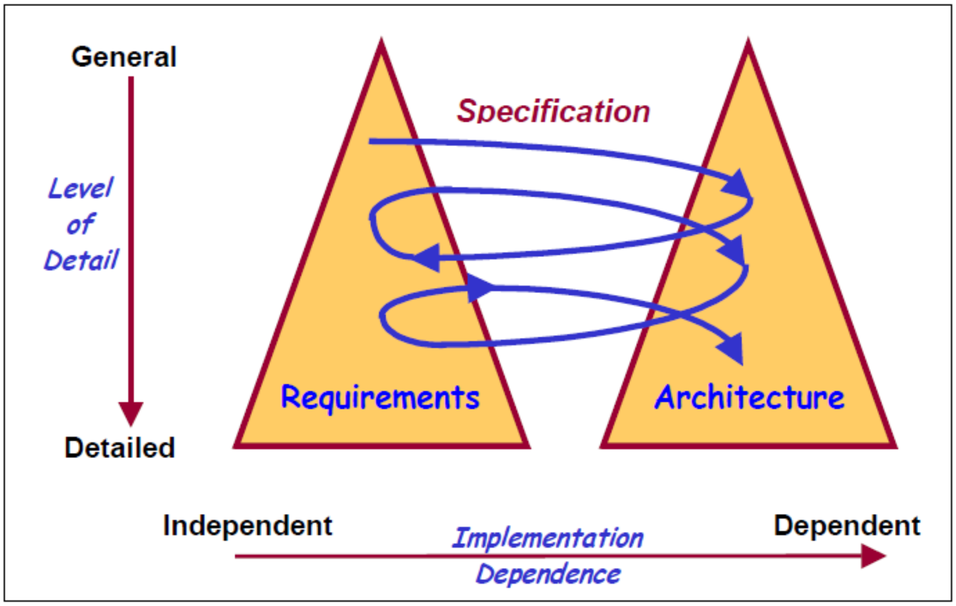


Figure 3.3: The “Twin Peaks” Model
(Nuseibeh, 2001)

3.2.4 Evaluating software architectures

An evaluation method with good trade-off analysis capability that incorporates trade-off analysis, sensitivity analysis, and risk management is necessary in delivering an acceptable solution (Zhu,2005).

ATAM is a structured method that aims to provide repeatability in the analysis of software architectural design. The method characteristically emphasizes the anticipations and participation of various stakeholders as contributors in the analysis and evaluation of architectural design with specific expertise and various specific quality-related quality concerns (Montenegro et al. (2017).

Bass et al. (2013) documents the Architectural Trade-off Analysis Method (ATAM) as one of the methods that can be used to evaluate the architectural design. The ATAM is one method by which the proposed architecture will be evaluated. The (ATAM) is a risk mitigation process that aims to develop or choose the most suitable architecture for a software system. Bass et al. (2013) explains ATAM as a process that brings together stakeholder concerns, architectural theories (approaches, patterns and styles) with architectural decisions to evaluate the architecture.

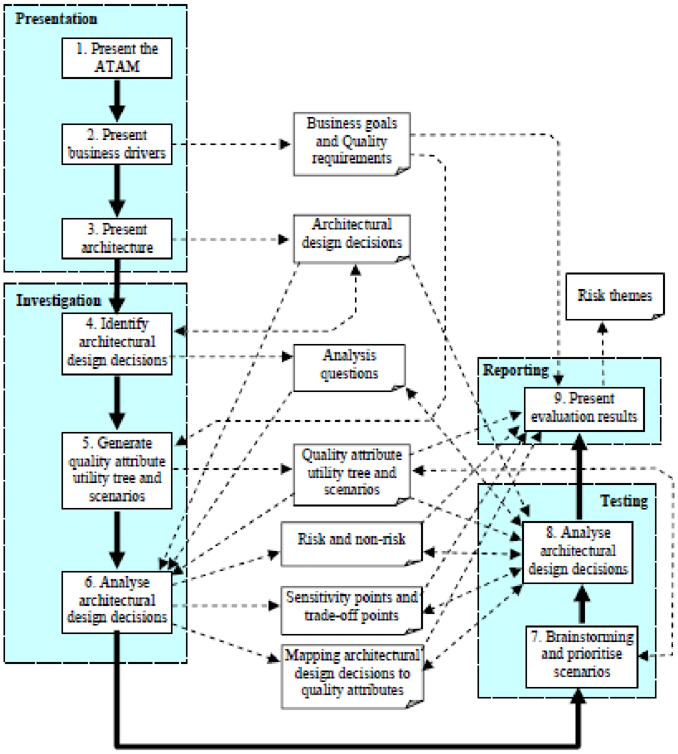

Presentation
1. Present the ATAM
2. Present business drivers
3. Present architecture
Investigation
4. Identify architectural design decisions
5. Generate quality attribute utility tree and scenarios
6. Analyse architectural design decisions
Business goals and Quality requirements
Architectural design decisions
Analysis questions
Quality attribute utility tree and scenarios
Risk and non-risk
Sensitivity points and trade-off points
Mapping architectural design decisions to quality attributes
Risk themes
Reporting
9. Present evaluation results
Testing
8. Analyse architectural design decisions
7. Brainstorming and prioritise scenarios

Figure 3.4: ATAM

(Adopted from Zhu, 2005)

According to Colquitt and Leaney (2007), the ATAM process (Figure 3.4) is comprised of the following stages:

3.2.4.1 Presentation

a) *Present the ATAM* - A description of the ATAM method is made to the stakeholder representatives including customers, the architect, user representatives, administrators, managers, testers (Colquitt & Leaney, 2007).

b) *Present business drivers* - The business goals are presented to the evaluation team i.e. the motivation behind the development project and what will be the primary architectural drivers. This includes high availability and security (Colquitt & Leaney, 2007).

c) *Present architecture* – According to Colquitt and Leaney (2007), the architects describe the proposed architecture, focusing on how it addresses the business drivers, the metrics, standards, models and approaches used to meet the drivers.

3.2.4.2 Investigation and analysis

This process involves identifying architectural approaches, generating quality attribute tree and analysing architectural approaches. In identifying architectural approaches, the architects identify applicable architectural approaches. These approaches play a part in design and are not part of the matter that is analysed (Montenegro et al., 2017).

Generating the quality attribute utility tree involves eliciting quality factors from stakeholders. These “utilities” include performance, availability, security and modifiability (Montenegro et al., 2017). The factors or features elicited from stakeholders are specified down to the level of scenarios, annotated in terms of the inputs / stimuli and outputs / responses. After identification, scenarios are prioritized, refined and represent user goals.

In analysing architectural approaches, the high-priority features or factors identified in the utility tree are analysed together with the architectural approaches that address those factors. For instance, an architectural approach that targets performance goals would be subjected to a performance analysis. Colquitt and Leaney (2007) propose that in analysing architectural approaches, scenario walkthroughs are used to convince the architectural approach as appropriate in meeting the attributes to specific requirements. The highest-ranking scenarios are used to explain the architectural decisions that had to be taken during the architectural design and refinement targeting, to deliver each of them.

3.2.4.3 Testing

a) *Brainstorm and prioritize scenarios* - Using the scenarios generated in the utility tree step, a larger set of scenarios is elicited from the entire group of stakeholders. This set of scenarios is prioritized through a voting process involving the entire stakeholder group.

b) *Analyse architectural approaches - Architectural* approaches are analysed again, paying attention to the highly ranked scenarios from the brainstorming sessions which are considered as core test cases for the analysis of the architectural approaches determined to this point. This process may yield additional architectural approaches, risks, sensitivity points and trade-off points that must be incorporated and documented.

3.2.4.4 Report and present results

According to Colquitt and Leaney (2007), the ATAM team concludes work by presenting findings to the stakeholders and write a report giving details about the information collected in the ATAM. This information provides details such as the architectural styles, scenarios, attribute-specific questions, the utility tree, risks, sensitivity points and trade-offs. This report is elaborated by Begum, (2018) as a report that provides detailed information including any proposed mitigation strategies against the risks that the process unearthed.

3.3 Research design

This research is designed around the “Design and Creation” project model (Oates, 2006). The pathway followed in this research is illustrated in Figure 3.4. The “Design and Create” model (Oates, 2006) is built around a framework of “6Ps” namely purpose, products, process, participants, philosophical grounding / paradigm and presentation. These “6Ps” are briefly explained in the following subsections.

3.3.1 Purpose

This research investigates impersonation in online assessments at Higher Education level, to analyse stakeholder concerns with regards online assessments, to design and create a software architecture description that discounts impersonation in those online assessments.

3.3.2 Products

This is a description of the expected and unexpected outcomes of the research project Saunders et al. (2015). The product of this research is a software architecture description for an online assessment system that reduces student impersonation. The product is expected to be a blueprint design for a secure online assessment system that reduces opportunities for impersonation to happen.

3.3.3 Process

Sekaran and Bougie (2016) explains that the research process reflects the conceptual framework of the research, the methodology applied, the strategy used to conduct the research and all the processes by which data is collected, analysed and interpreted to draw conclusions.

3.3.4 Participants

This section specifies the role played by the researcher and other stakeholders in this research project. As an emic project, the researcher was directly involved in the process and actively performed tasks e.g. the literature reviews to gain a background understanding of online assessment systems and the threats to their security, focusing on impersonation. The researcher performed the activities discussed in Section 3.6 to Section 3.12. Stakeholders that include students, faculty, line management and higher level institutional administrators provided information about online assessment systems and evaluated the proposed design. The participants in this research are described in Section 3.6.2.

3.3.5 Philosophical grounding

The term “research philosophy” sums up the system of beliefs and assumptions about the development of knowledge (Sekaran & Bougie, 2016). These assumptions shape up the way that the researcher understands the research questions, the methods they use and how they interpret their findings. According to Saunders et al. (2015), the assumptions basically fall in the categories of ontology, epistemology and axiology.

3.3.5.1 Ontology

Ontology is a reflection of the nature of reality (Saunders et al., 2015). Ontological assumptions influence the way in which the researcher focuses the research and the way the researcher views the research subjects, values and interprets the results. This research is a phenomenological study with an ontology that is multiple / plural as it targets to capture the different realities of stakeholder’s living experiences, views and concerns on impersonation and how the different stakeholder roles believe it can be reduced in online assessments. The researcher is involved in online education and assessment and holds a reality that may differ from the views of other roles in the online assessment system.

Through the research processes, the researcher explores multiple perspectives and contextual situations, for example, the reality from the standpoint of the student and the different realities from the faculty, institution and industry at large. This ontological standpoint justifies the choice of qualitative data collection and qualitative data analysis in this research project. This research aims to acquire an in-depth and complete understanding of the phenomenon of impersonation in online assessments.

3.3.5.2 Epistemology

This qualitative study seeks to deepen understanding of the nature of online academic assessment, academic malpractice, placing focus on impersonation in Higher Education online assessments. The study uses a subjective, plural truth approach that is context-based in the gathering of knowledge through the design of a solution to the joint evaluation of a software architecture with stakeholders. Structured interviews, document analysis and overt direct observation are the tools selected to collect the data from stakeholders and in evaluating the architectural design in iterative cycles.

3.3.5.3 Axiology

The researcher is actively in the online education career. Through application of the ethical practices stipulated for good research and subscribed to by the CPUT, the researcher did not impose preconceived ideas on the participants. This is reflected in the Questions and questioning style. The Questions for each stakeholder group are presented in Appendix A of this thesis.

From an axiological perspective, it is submitted that the researcher, as a practitioner, was subjectively immersed in and thus influenced the study. As this was an emic study, the researcher acknowledges the presence of some bias or subjectivity in terms of how the data gathered are filtered through the consciousness of the researcher and interpreting or understanding the experiences of others of how impersonation can happen in online assessments, the frequency of occurrence and the effectiveness of mechanisms that institutions employ as they attempt to reduce or combat it. It is admitted that utmost caution was necessary to ensure that the researcher’s experience, encounters and prior knowledge did not influence the final outcome.

To reduce bias on the outcomes, interpretations and conclusions, the researcher engaged many real-life practitioners in online assessment as subject matter experts e.g. faculty staff and academic quality managers to objectively review facts, challenge assumptions, opinions findings, and conclusions using discussion and brainstorming.

3.3.6 Presentations

The findings of this research shall be presented as a thesis to the Information Technology Department within the Informatics and Design Faculty.

3.4 Choice of the design and creation research paradigm

According to (Oates, 2006) “research is a human undertaking that is shaped by human reasoning”. This software engineering research project aims to design and create, at low cost, a software architectural definition for online assessments that addresses the problem of impersonation while causing minimum disruption to the student. This research could not be adequately serviced by one paradigm. In order to conduct this research, different paradigms had to be combined with the design and create paradigm. Following Oates (2006), a combination of paradigms can be employed as long as the combination is “explained and justified”.

The problem of impersonation in online assessments was researched using a combination of interpretive and perspectives and critical research paradigms at two different institutions to develop an understanding of the reality of impersonation in academic assessments and to develop a software architecture based solution. The Design and Creation paradigm was selected to design and create a software architecture description that could deliver secure online assessments.

This design and creation research paradigm was selected for this project because the project aims to deliver a new artefact in the form of a system design for secure online assessments. The Oates Model (Oates, 2006) is one of the specific software engineering models that can guide software engineering design projects.

The choice of the Oates model for this design and creation research is justified for several reasons as follows:

The Oates model accommodates and incorporates the researcher's experience in assessments, earlier research work and a high-level of stakeholder involvement. This makes the paradigm favourable from the ontological and axiological reasons.
The project requires soliciting of qualitative information from various sources and stakeholders using a range of techniques and tools. Tools for qualitative data gathering such as interviews and observation are availed in the design and creation paradigm.

The Oates Model provides a good pathway or guide through the research process and also the techniques that can adequately meet the philosophical and practical demands of this research project.

The design and creation paradigm are well suited to the interpretive nature of the research design. This research collects information from various stakeholder groups and interprets it to gain insight into the concerns and expectations of each group, as well as the online assessment experience. This understanding avails to the researcher, knowledge of potential ways in which online assessment systems may be enhanced or hardened to address impersonation fraud.

Figure 3.5 shows the Oates model and how it was adopted to guide this research project. The highlighted boxes indicate the pathway through the model this research followed:

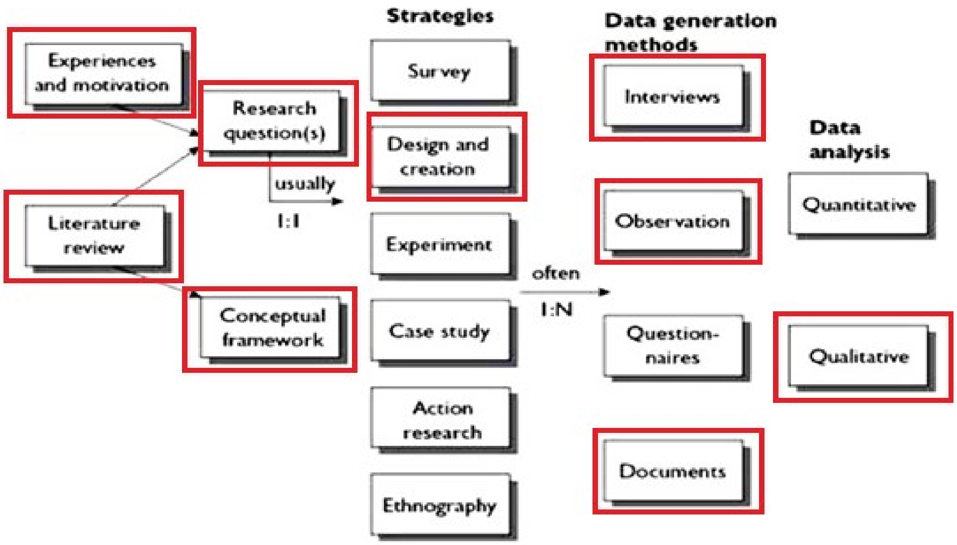


Figure 3.5: The Oates Model
(Oates, 2006)

3.5 Research approach

This research takes a qualitative approach to explore the phenomenon of academic impersonation. As Mack et al. (2005) describe qualitative research, it uses flexible instruments in an iterative manner to elicit and categorize participants' responses to questions. Semi-structured methods in the form of in-depth interviews, focus groups and overt process observation are employed as the data collection methods as they facilitate change and improvement in action (Mack et al., 2005).

The Data Analysis approach adopted in a qualitative research aims to identify and describe variation, describe and explain relationships between entities and processes. In this research, qualitative methods were used as they facilitate capturing and analysis of individual experiences, group norms and group expectations. The analysis of data in this project follows the inductive reasoning approach. According to Dudovskiy (2016) the inductive reasoning approach means following a clear, logical pathway from observing, to establishing patterns, and formulating a theory or conclusion based on the facts amassed during the steps (Figure 3.6).

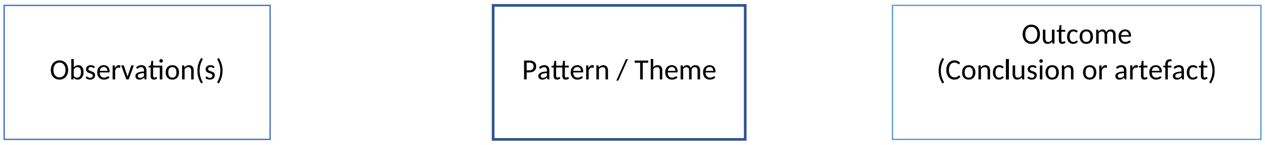


Figure 3.6: Inductive research approach
(Dudovskiy, 2016)

The inductive approach was used in this research because of the following features (Mack et al., 2005) and reasons:

This is a qualitative research project. The project seeks to draw concerns and viewpoints from stakeholders and use them in developing a solution to the problem of impersonation in online assessments.

Inductive research offers the necessary flexibility for such a project. As the data collected is expected to be subjective and qualitative, flexibility in data collection, transcription and analysis are necessary for the collection of rich data and for meaningful conclusions to be drawn.

Inductive research provides an interpretative perspective. This type of research demands the researcher to develop an understanding of user experiences and perceptions.

The project has an exploratory perspective focused on identifying and understanding stakeholder concerns.

3.6 Research strategy

Batyuk (2018) depicts research strategy as a systematic plan of steps that the research follows, in order to produce valid results while satisfying the constraints imposed on the project, such as costs and time. This research strategy adopted for this project was chosen specifically because this research project is stakeholder driven (Oates, 2006) and must deliver a solution that balanced a range of constraints such as stakeholder priorities, cost and time constraints.

The research strategy adopted is comprised of the following series of steps; Define scope and context, identify stakeholders, engage stakeholders, capture stakeholder concerns, define the architecture and evaluation of the software architecture. Figure 3.7 presents the research strategy for this project.

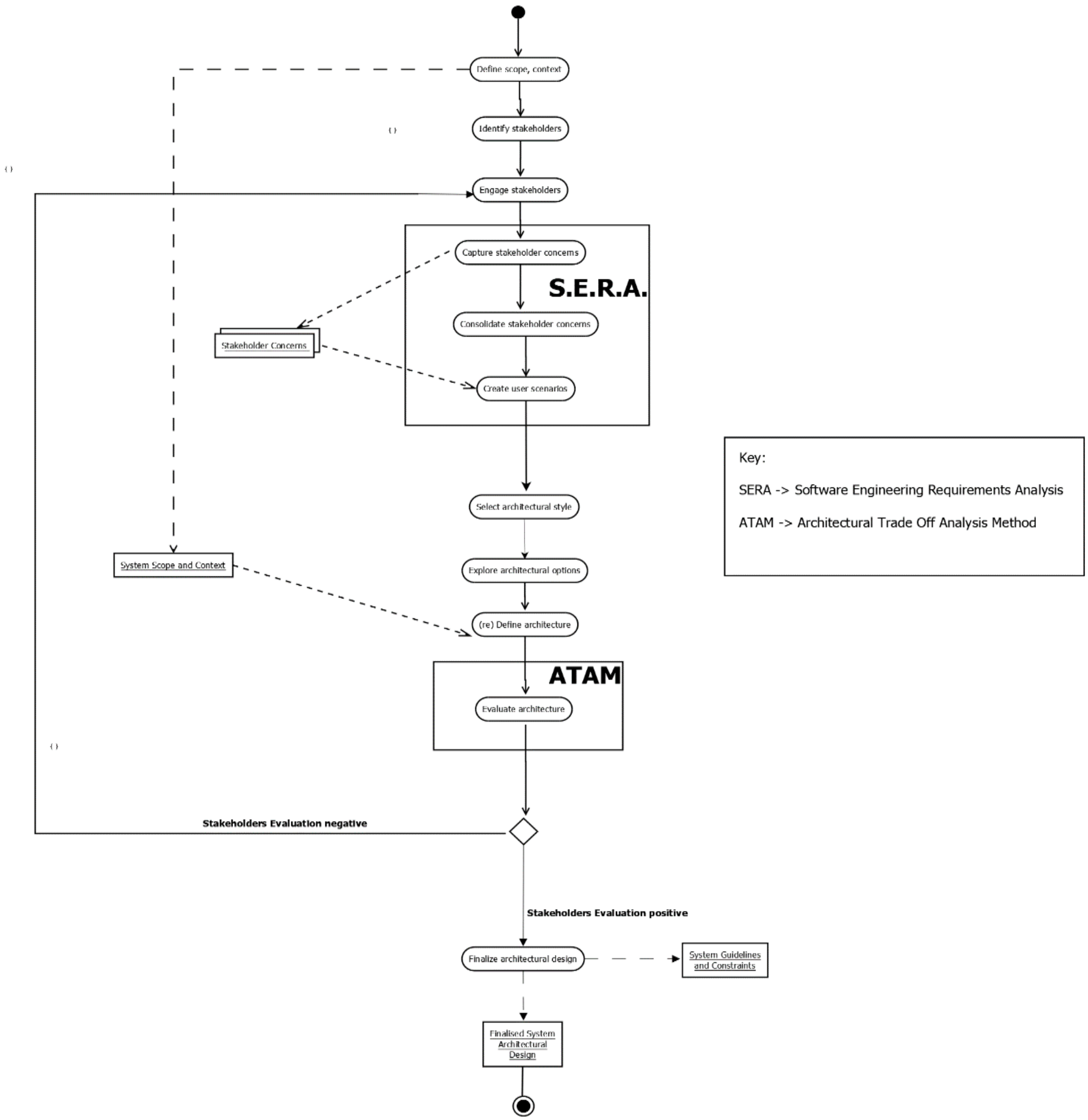

Define scope, context
Identify stakeholders
Engage stakeholders
Capture stakeholder concerns
S.E.R.A.
Consolidate stakeholder concerns
Stakeholder Concerns
Create user scenarios
Key:
SERA -> Software Engineering Requirements Analysis
ATAM -> Architectural Trade Off Analysis Method
Select architectural style
System Scope and Context
Explore architectural options
(re) Define architecture
ATAM
Evaluate architecture
Stakeholders Evaluation negative
Stakeholders Evaluation positive
Finalize architectural design
System Guidelines and Constraints
Finalised System Architectural Design

Figure 3.7: Research strategy
(Adapted from Mackenzie, 2014)

3.6.1 Define scope and context

When a software development project begins, a scope for the project is defined by the project sponsor or customer. According to Batyuk (2018), the scope sets the parameters that guide the rest of the project such as the budget, time, required features, general capabilities, and acceptable risks related with the project or its outcomes. In this project, this scope definition activity provides a clear definition of the online assessment system in terms of its boundaries, interfaces, inputs, outputs, and positioning or context.

Batyuk (2018) goes on to emphasize that this activity clarifies the needs, goals and vision of the academic institution or business. The activity also identifies and clarifies the business drivers i.e. the issues that are focal in the business, the organizational strategy of the institution and the elements that must be included or excluded in this academic research i.e. project delineation.

With these factors defined, software engineering techniques and tools are used to elicit concerns from the stakeholder communities.

3.6.2 Identify stakeholders

The ISO standard (2600:2) identifies a stakeholder as:

"any individual or group that has an interest in any activity or decision of an organization or system".

It is important to identify stakeholders and ensure that their stakes or interests in the organization or system are as clear as possible. Stakeholders' concerns are the determinants of success in any organization or system. For this research, a practical technique proposed by Gama (2017) was used.

According to Gama (2017), stakeholder identification yields the names of representative people with whom the project may be undertaken. The stakeholders for online assessment systems are many and these stakeholders hold various interests or concerns in the system or its products. Gama (2017) proposed that the first step was to identify and categorize the stakeholders into groups' according to their roles in the system, business position or anticipated concerns.

Representation from each group is then sampled. This simplifies the process and enables the concerns of each group to be clarified and consolidated. A stakeholder list is prepared to document the stakeholders, their roles, and the representatives.

To facilitate the data collection and subsequent data analysis, grouping the project's stakeholders into different categories was essential. For each category, different interview themes targeting specific focal points formed the basis of the interviews.

The stakeholders identified in the online assessment system fell in at least one of the following categories i.e. students group, parenting group, faculty group, quality management group, information systems group and policy making group.

3.6.2.1 Student group

This group describes current students and "recent former students" who are recent graduates from online education courses. This stakeholder group was chosen to provide first-hand information about the assessment experience, the assessment environment, student motivations to cheating and how cheating happens in online assessments. Generally, the group was targeted to obtain answers to SQ1 and SQ3 through structured interviews.

3.6.2.2 Parenting group

The parent stakeholder group comprises biological parents, foster parents and guardians of students. The group was chosen because some of the research subjects were under legal adult age and the parents and guardians were included to give consent for the minor participants to partake in the research project. This group incidentally also had parents who were also studying towards Higher Education and occupational qualifications online. These participants benefitted the research with their rich and mature appreciation of the research and its potential value and implications to education, work and society.

3.6.2.3 Faculty / Educator group

This group describes current academic teaching and other "practitioners" in education such as teaching &training administrators and student advisors. This group of stakeholders interact with students regularly during the learning and assessment processes. In the online assessment system, the roles of faculty largely revolve around administering virtual, distributed learning experiences where learners are geographically spaced and reachable via various computer and Internet technologies. The faculty stakeholders group is involved in content and assessment development e.g. authoring, the construction of quizzes and tests banks, their on-line delivery, assessment invigilation, grading, moderation and reporting.

3.6.2.4 Quality management group

The quality management group comprises of stakeholders such as program leaders, academic quality managers, heads of departments, deans and registrars. This group takes a keen interest in quality measures of education and assessments i.e. content quality and the modalities of assessment delivery. Quality managers pay attention to verifying performances of the assessment system at management level i.e. determine whether the online system delivers the correct assessment to the correct student groups, at the correct time, in the correct format and with minimum errors. These stakeholders were chosen because they oversee the operation of faculty staff and authorize processes such as interventions by faculty staff in the assessments.

3.6.2.5 The information systems group

The information systems group comprises experts in the field of Informatics who perform technical tasks such as developing computer-based solutions to business problems, administering the assessment system, monitoring system performance, processing requests for system change and enhancements and effecting corrective action as needed.

In the online assessment system, these stakeholders also pay keen attention to ensure the correct execution of the identity management functions, the security of the system through identification, authentication, authorization and accountability. This group of stakeholders was chosen to provide insight into what happens “behind the scenes during online assessments”.

3.6.2.6 The policy makers group

This stakeholder group includes the institutions that own the systems, examinations councils and bodies, society, government departments, school heads and principals, and industry. The policy stakeholder group is regulatory by nature and has a very big influence on the operations of the entire academic institution as organizers of educational, financial and human resources. These stakeholders do not directly partake in the online system, but consume information delivered by the online assessment such as enrolments, pass rates, and other performance statistics.

Policy makers were required in this study because some members of this group access the system from time to time, though mostly in a read only capacity mode, for instance to pull reports. To obtain a complete understanding of assessment environments and to maintain system security and data integrity, users had to be involved and their concerns taken into account.

3.6.3 Engage stakeholders

The identified stakeholders were engaged in order to obtain knowledge of their interests and concerns. According to Oates (2006) and Bass et al. (2013), a stakeholder-centred process is important as it provides clarification of stakeholder needs, expectations and facilitates the elicitation of system requirements. Engaging stakeholders in the project includes creating a working relationship with them. Establishing this relationship with stakeholders is vital in clarifying the scope, context and positioning of the system within the organization.

According to Oates (2006), establishing rapport with the stakeholders is vital so that the nature and extent of the way the system affects them are determined. Stakeholder engagement and involvement in data collection activities took place through interviews and during observation that was structured and aligned to this stakeholder classification. Table 3.1 summarizes the participation of the various stakeholder classifications in the research.

Table 3.1: Participants in data collection

Stakeholder Group	Number of participants
Students	85
Parents	20
Faculty educators	77
Quality management	21
Systems group	17
Policy group	9

3.6.4 Capture stakeholder concerns

For a software development project to succeed, developers need a clear understanding about the requirements of the stakeholders, making it vital for the stakeholders to understand their role in specifying their requirements. Clarification of the project goals is important so that they can participate effectively in the project. Oates (2006) submits that stakeholder participation in the project means clarifying the concerns of the stakeholder, the value / priority rating of the concern to the stakeholder (product metrics of performance evaluation and establishing accountability and measures of success that the stakeholders will use to validate possible changes.

Product metrics help to provide insight into the design and construction of the software that is being built. Bass et al. (2013) suggests that the activity of capturing stakeholders' concerns should end by consolidating the concerns of the stakeholder groups so that the functional features of the system are clarified and documented. This rests largely on the creation of scenarios by the developers and stakeholders from the stakeholder concerns. Scenarios form the core tool in designing, presenting, analysing, and reviewing of the design artefacts (Gama, 2017).

3.6.5 Define the architecture

According to Bass et al. (2013), defining the software architecture from elicited stakeholder concerns requires a systematic combination of the theory of software architecture, architectural decisions within the defined system scope and stakeholder concerns to create an architectural definition. The theory of software architecture provides tools and techniques such as the architectural plan, approaches, styles, and the stakeholders set the scope and the range of concerns that define the expected final product (Oates, 2006).

3.6.6 Evaluation of Software architecture

After developing a software architecture, it is evaluated in the context of the scope and context of stakeholder concerns or requirements (Gama, 2017). Many techniques such as McCall's 11 Factor Model as explained by Ouhbi (2018), provide metrics against which a design can be evaluated. The McCall model classifies the 11 metrics in 3 broad classes. Product operation factors that incorporates the correctness, reliability, efficiency, integrity, and usability of a software artefact. The product revision factors include the maintainability, flexibility, testability of the software product and product transition factors. These jointly cover the portability, reusability, and interoperability of the software.

3.7 Sampling

For this research, samples had to be drawn from students, parents, faculty and management. Palinkas, Horwitz and Green (2015) defines sampling as "… the process of drawing a set of representative elements from a population for use within a study. The target of sampling is to select and work with a data set that is small enough to be manageable for analysis purposes, but large enough to ensure that conclusions made from studying the sample can be generalized for the entire population…"

In this project, *purposeful sampling and snowball sampling* are the sampling techniques that were chosen to select participants from the stakeholder communities.

3.7.1 Purposeful sampling

Purposeful sampling was chosen because it allows the selection of participants basing on some value-based criteria that is considered suitable for the research task (Palinkas et al., 2015). In this research, participants were selected purposefully in light of their concerns and roles they play in the creation, management, administering, and conduct of online assessments. Stakeholder groups in an online assessment system include heads of institutions, heads of departments (or faculties), academic quality managers, educators, assessors, invigilators, system developers, administrators and students.

3.7.2 Snowball sampling

Snowball sampling incorporates such sources when they come recommended by other subjects of the research. In Higher Education, so many people play a role in assessment and institutions have varying practices or protocol. This method gave access to more information in the Higher Education assessment system.

3.8 Data generation methods

As a study that aimed to collect different concerns from diverse stakeholders, this study used different methods for qualitative data collection. The data generation process aimed to collect information from existing body of literature and the concerns of the stakeholders. Following the work of Nuseibeh (2001), data generation and the development of a software architecture were carried out concurrently. Data generation took place as a continuous process in two major phases i.e. in collecting stakeholder concerns from which the specification of a software architecture would be created and in evaluating the software architecture description.

In the first stage, the requirements engineering approach was used to accurately gather and refine data from the stakeholders. According to Laplante (2017), the requirements engineering process shown in Figure 3.7 (S.E.R.A) is magnified and shown in Figure 3.8.

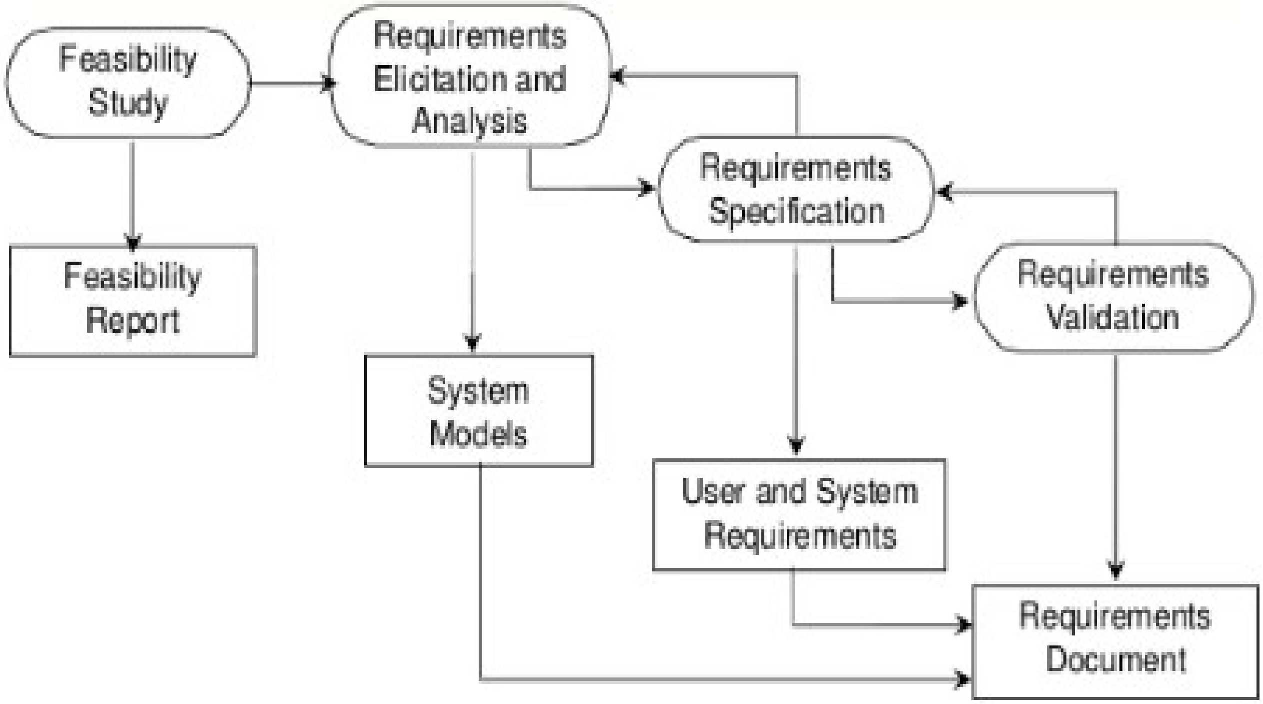


Figure 3.8: Requirements engineering
(Laplante, 2017)

As a qualitative research involving diverse stakeholders, a combination of interviews, observations and document reviews were employed in the requirements elicitation and analysis step to collect information about online assessments and academic impersonation.

The data collected using these tools were combined with the data collected in the pre-study and from the literature review to create the first candidate software architecture. The candidate architecture was subsequently used in Architecture Trade-off Analysis Method (ATAM) sessions to solicit more detailed information from stakeholders. These two techniques of fact gathering were used in iteration to obtain a detailed understanding of stakeholder concerns, priorities and in evaluating each candidate architectures throughout the project.

As Figure 3.8 shows, the specific stages that were used to elicit or acquire data from the stakeholders. The main methods employed were structured interviews and focus groups involving volunteering participants, document reviews accessed with the consent of institutions and overt observation of online assessment processes. These processes are elaborated in the following subsections.

3.8.1 Interviews

Mann (2016) describes interviews as conversations in the form of questions and answers that researchers can use to obtain information. In this research, interviews were used to engage willing, volunteer stakeholders to elicit system features or requirements. Each interview was structured and comprised of a combination of open-ended and close-ended questions. For ethical reasons, interviewers were not required or requested to identify themselves by name, instead, each interviewee was kept anonymous and was identified by post within the institution or the role they played in assessment processes (Turner, 2010).

The objectives of the research, storage of materials and the disposal of the materials upon completion of the academic process were clarified to each participant. Subjects were informed of their rights (Loiselle, 2008) to withhold answers to questions they found sensitive, risky to their person or employment and the right to withdraw their participation at any time they find it necessary or convenient to do so.

Turner (2010) explains that open-ended questions permit the interviewee to provide answers in their own words and in more depth than close-ended questions that require interviewees to select an answer from a limited domain of possible answers. Following the guidance of Lambert and Loiselle (2008), in this research, interviews took the following forms:

3.8.1.1 Individual interviews

As suggested by Lambert and Loiselle (2008), wherever and whenever possible, stakeholders were scheduled for interview one-by-one in a private place. Without exceptions all management and senior stakeholders were interviewed individually. Participation in paired and focus group interviews was purely optional to the participants as these forms of interview take away the anonymity of the participants (Wilson et al., 2016; Lee et al.,2018).

3.8.1.2 Paired interviews

Co-workers at operational level such as educators, assessors and invigilators had the option of attending interviews in pairs. This option was made available prior to engagement in the interview and communicated by management as part of the formal introduction of the project to staff. This preference was confirmed by the researcher before the interviews commenced. According to Wilson et al. (2016) the objective behind paired interviews was to reap additional benefits such as clarification, reliability checking at peer level, alternative opinions, contradictions, or amplifications.

3.8.1.3 Focus group interviews

Stakeholders of similar interests, functional roles, or ranking were given the option to be engaged in group interviews and brainstorming sessions under supervision and moderation of the researcher, following the guidelines of Lee et al. (2018). This method promoted the cross-pollination of ideas, assisted in clarification and prioritization of needs within the group, and provided the members of the stakeholder community with space to support each other. The focus group pre-cursed the individual interviews and thus helped in the formulation of more specific and relevant questions. This made the interviews more targeted and easier to manage in terms of time and location. Educators, teaching assistants and student support groups within the stakeholder community were engaged in focus groups because of the huge number of these participants in the academic assessment system.

3.8.1.4 Remote or distance interviews

Mantoro and Johnson (2019) qualify long distance or remote interviews through the telephone, Voice over IP (VOIP), videoconferencing through Skype™ as ways to augment face-to-face interviews. Remote interviews were used in this research to include stakeholders who were not accessible easily. The subjects used in this research were stationed in the ten provinces of South Africa’s at forty-six branches of one of the institutions used in this research.

Some of the participants were based in Mbabane Eswatini. For reasons of completeness and economy, telephonic interviews, Skype™ and videoconferencing communication tools had to be used to conduct interviews with willing participants who could not be reached for face-to-face interviews. These technologies were used because they provide a method to cater for the different types of interview i.e. individual, pair, and focus group interviews.

3.8.2 Document review

Bowen (2009) discusses the literature relating to the conduct of online assessment e.g. procedure manuals as sources of information. In this research, willing heads of faculty, educators and other stakeholders were permitted access to documented online assessment procedures, fraud or other violation cases and outcomes for the researcher to review. This fact gathering exercise afforded the researcher more insight into what happens within the institution in the conduct of online assessments. Further, this data generation method was chosen because of its potential to shed light on the prescribed requirements, needs, actions, and measures that should take place during assessments according to the rules and regulations that apply to online assessments.

3.8.3 Observation

Dudovskiy (2016) presents observation as a research instrument that enables the researcher to gather data from within an environment, situation, or system of interest by closely watching processes, or interactions within the process or system. In this research, overt, structured, and scheduled observation were used to collect data during assessment sessions. Institutional staff, students and parents were informed in advance and their consent was sought before the observation commenced. Observation was chosen as a data generation method because observation gave the benefits of providing first-hand information to the observer (Quinlan, Babin and Carr, 2019). Observation offered the researcher the benefit of a “complete view” of the online assessment system and its operation in real life (Curdt-Christiansen, 2019).

Observing invigilated online assessments gave a basis for refining other research tools and actions, for example, observations clarified the researcher’s understanding of online assessment activities and processes. After observing, the researcher formulated more specific interview questions and could discern differences between the prescribed practice in the conduct of online assessments, and the manner in which online assessments happen in reality.

3.9 Data transcription

The detailed, thick and rich data Flick (2010) collected from interviews and focus groups through audio recordings and note taking was transcribed using the comprehensive transcription protocol as described by Bokhove and Downey (2018). It was not anticipated that the data collected would be overly ambiguous or extremely varied, making comprehensive transcription protocol usable and hence its selection for this project. The comprehensive data transcription protocol requires the researcher to paraphrase content manually or using speech recognition software. Dudovskiy (2016) argues in favour of this protocol and highlights that the protocol is favourable for the methods chosen for data transcription and qualitative (subjective) analysis by techniques such as thematic analysis, content analysis and inductive deduction.

3.10 Data analysis methods

Alhojaila (2012) explains that the data generation methods of interviews, document reviews and observation yield qualitative data in the form of words, observations, symbols and graphics.

Flick (2010:14) explains that qualitative data analysis aims to "develop as thick, as rich and complete an account of the phenomenon under investigation as possible. Analysis of such data typically happens simultaneously during data collection."

This study acknowledges and attempts to understand multiple realities (subjective realities of participants or stakeholders) of impersonation in online assessments and therefore utilizes qualitative research methods situated in the interpretivist paradigm to construct an understanding.

3.10.1 Thematic analysis

As this was an emic study, data analysis progressed concurrently with data gathering. Using the approach suggested by Belotto (2018), the following sub-processes were chosen for the qualitative analysis of collected data:

a) *Focusing the analysis* – The researcher focused analysis by intently studying the recordings taken from interviews, focus groups and ATAM sessions, referencing research notes from focus group and observation sessions. Recurring points, terms, concepts, aspects, concerns and views about issues related to online assessments were from each stakeholder group or individuals were noted.

Close attention was paid to these as pointers to more specific issues or concerns for the stakeholder group. From these reviews, key questions, terms and issues emerged and considered as candidate themes for the stakeholder group in question. For instance, the need for robust identification and continuous authentication of students featured as a prominent concern among faculty staff, while cost and privacy issues featured prominently among the policy makers, students and parents' groups.

b) *Coding and indexing* – Themes and patterns were searched for around the noted concerns and issues. These themes were then coded to facilitate easy data organization, summarization and quick retrieval. The collected data was coded with reference to the stakeholder group and the research sub-question. Within each stakeholder group, the data collected was further coded with reference to specific concerns such as Privacy, Security, availability, reliability, cost, compatibility with Learning Management Systems (LMSs), usability and speed or response. These concerns were classified as follows:

Security Concerns E.g. Identification of student (at start of assessment), Authentication of student identity (at start of assessment), authentication of student identity (during the assessment) – i.e. presence validation, identification of student (at the completion of assessment), Authentication of student identity (at completion of assessment) and confidentiality and privacy.

Cost Concerns e.g. cost effectiveness metrics and measures

Usability Concerns e.g. The quality of student experience and compatibility with LMS

Compatibility with LMS e.g. operating speed, reliability, scalability and availability

Effectiveness concerns including the likelihood of authentication success i.e. system effectiveness, scalability, reliability, availability and speed.

c) *Identifying patterns* – Themes and patterns in the data needed to be identified and analysed to provide meaning and connection to other data. This step involved identifying patterns within institutions at centre or branch level and between branches.

Commonalities across branches, stakeholder groups and between the organizations used in this research were also identified at the stakeholder and institutional levels.

d) *Interpretation of the data* – In this process, the researcher sought the meaning of the data gathered by condensing the identified themes and patterns and abstracting the collected data. The primary methods used to interpret the data were content analysis, thematic analysis and analytical induction.

3.10.2 Content analysis

This data analysis technique aims to determine the presence, frequency and prevalence of keywords, phrases and other language devices. This type of analysis benefits from good classification and indexing of data collected. The method described by Braun, Clarke and (2018) works by tallying the frequency of occurrence of the keywords and phrases. Using this method provided insight into common interests, thrust and focus among the stakeholders or stakeholder groups using the categories listed in Table 3.1.

3.10.3 Analytical induction / Grounded theory

The researcher formed some meaning of the collected data using analytical induction. Through direct comparison of data collected from stakeholders at different institutional levels with different roles and within different institutions. This constant comparison facilitated the definition of categories, relationships between categories and the identification of patterns. This constant comparison continued throughout the study and enabled the identification of core categories.

These core categories formed the basis on which discussion in focus groups centred and upon which architectural designs were evaluated in ATAM sessions. The categories of privacy, security, availability, reliability, cost, compatibility, usability, scalability and speed were used determinants in trade-off analysis as an application of the Criteria Importance Theory (Orlov & Vishnyakov, 2017). This research was ultimately characterized by this iterative progression in which the researcher moved constantly between data collection and data analysis.

Ruhode (2016) submits analytical induction / grounded theory as a technique aimed to explain the data collected by inductively developing a theory from amassed data. Through coding, theories emerged, and the themes constructed into theoretical models that were compared with existing literature on topics such as architectural patterns, online assessment system features.

Themes were derived from within the data through inductive analyses and from the investigator's prior theoretical understanding of the phenomenon of impersonation, how it takes place and the methods that institutions employ to reduce the chances of it happening. According to Saunders et al. (2015), this process is cyclic and iterative. Each cycle creates more themes that move closer and closer to a desired result.

3.11 Solution Design

In developing candidate software architectures, the Feature Driven Development model was applied. This was used to interface the requirements provided by the user into features of the architecture as the requirements were realized over time. Each requirement was considered at two levels; individually and at a higher systems level to identify conflicts and potential fit.

The Criteria Importance Model Orlov and Vishnyakov (2017) was applied to rank and prioritize features and requirements to be incorporated in each iteration. The criteria included feasibility and suitability, simplicity, scalability and interoperability to evaluate and rank alternative designs.

Nawaz, Aftab and Anwer (2017) present Feature Driven Development (FDD) as a pragmatic, iterative, "client and architecture-focused" software engineering process that seeks to identify the features, i.e. functionalities and attributes that stakeholders in a system demand or expect from the system. In FDD, the features specified by the stakeholders are a source of requirements to software developers, hence they form the primary input into the planning process (Ambler, 2005). Research and development efforts focus on identifying, analysing, and understanding the system features or requirements as demanded by the stakeholders.

The primary target of software development is delivering or meeting these requirements in a pecking order that brings the most value to the stakeholders. Figure 3.9 shows the FDD model, emphasizing the role of stakeholder features and the iteration between design cycles that lead to the delivery of a product that meets the value of the stakeholder.

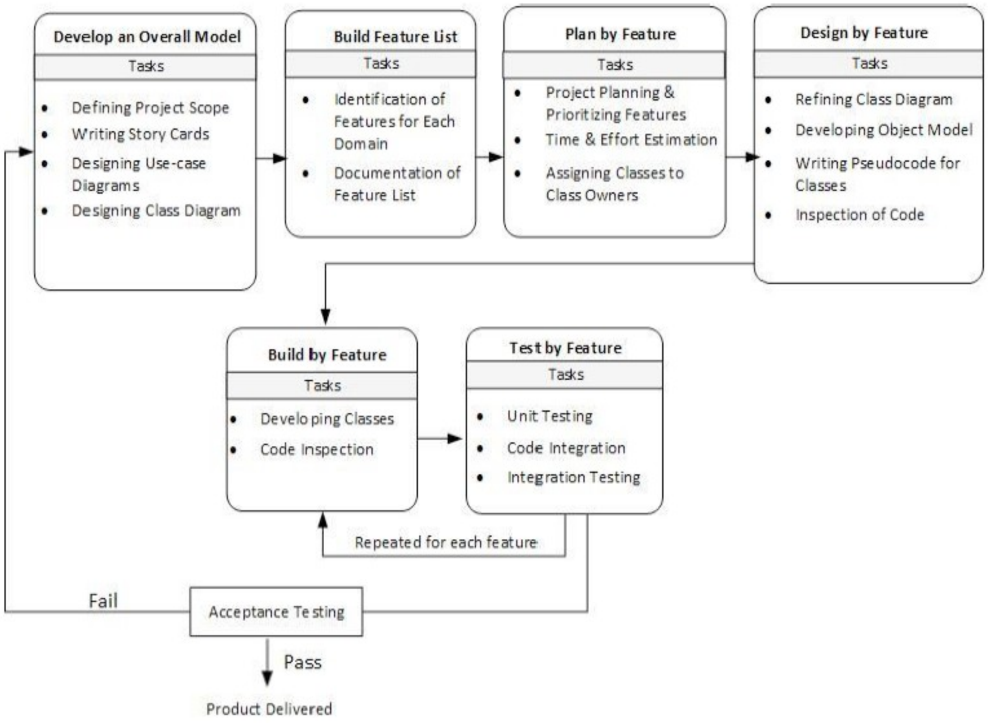


Figure 3.9: Feature Driven Development
(adapted from Ambler, 2005)

At the end of each FDD iteration, a working module is delivered and used to solicit feedback from the user and form a basis for any subsequent iteration (Nawaz et al., 2018; Saikiran & Simon, 2019).

Nawaz et al. (2018) explain that each iteration is comprised of the following stages as depicted in Figure 3.8 i.e. develop an overall model, build a features list, plan by feature, design by feature, build by feature and test by feature.

3.11.1 Develop an overall model

This involves walkthrough discussions between the developer and the client to determine and pin down the scope and context of the project (Nawaz et al., 2018). The scope is finalized between the developers and domain experts. And documented in scope documents, functional and non-functional requirements, class diagrams and use cases. In this project, the researcher engages the domain experts i.e. faculty staff and management in formal discussions and interviews to solicit project scope, contextualize the project, delineate the project and requirements, determine overarching requirements and constraints.

3.11.2 Build a feature list

The main activities are the creation and management of the features or requirements list. The identified requirements are categorised into feature sets which are used to refine the user requirements, associations between the requirements, and the different stakeholder groups (Saikiran & Simon, 2019).

3.11.3 Plan by feature

The features are prioritized so that in the early iterations, high priority features are addressed ahead of low priority features. Each feature is prioritized according to the business need, dependencies with other features and the complexities involved. According to Saikiran and Simon (2019), this stage ends with the deployment of feature sets to developers. The architectural features of the secure system are prioritized in line with the business case, and dependencies between the features taken into account when creating the software architecture. A project plan that details the subsequent design and reviews is formally submitted.

3.11.4 Design by feature

Nawaz et al. (2018) explain this stage as the stage that focuses on different activities such as the design of sequence diagrams, writing classes, evaluation and refining the overall model. This stage delivers the object model. In this project, a proposed software architecture design is created using the UML and presented the Architecture Trade-off Analysis Method (ATAM) sessions. The early design proposals are filed and used as starting points for succeeding iterations.

3.11.5 Build by feature

In this stage, the object model is implemented as design packages. The model is translated into program code. The program code is formally inspected and tested. The cycle ends with the delivery of a set of workable modules (Nawaz et al., 2018). Feedback from ATAM sessions is incorporated in the design, adding detail and clarity to the architecture. In each iteration, features are added, removed or edited in agreement with users and considering design constraints and principles. This research project concludes with the creation of a software architecture. The proposed solution is not implemented in the physical context, so no program coding or testing happens (Saikiran & Simon, 2019).

3.12 Evaluating the architectural design

This research aims to produce a software architecture solution for an online assessment system that reduces impersonation to the satisfaction of diverse stakeholders and quality attributes. As such, a set of concerns or quality attributes must be considered at the same time, some of which have inverse relationships and trade-offs imperative (Bass et al., 2013). Figure 3.10 shows the process flow of the ATAM method of architectural review combined with the Software Requirements Engineering Analysis as the technique that was used in this project for evaluating architectural design.

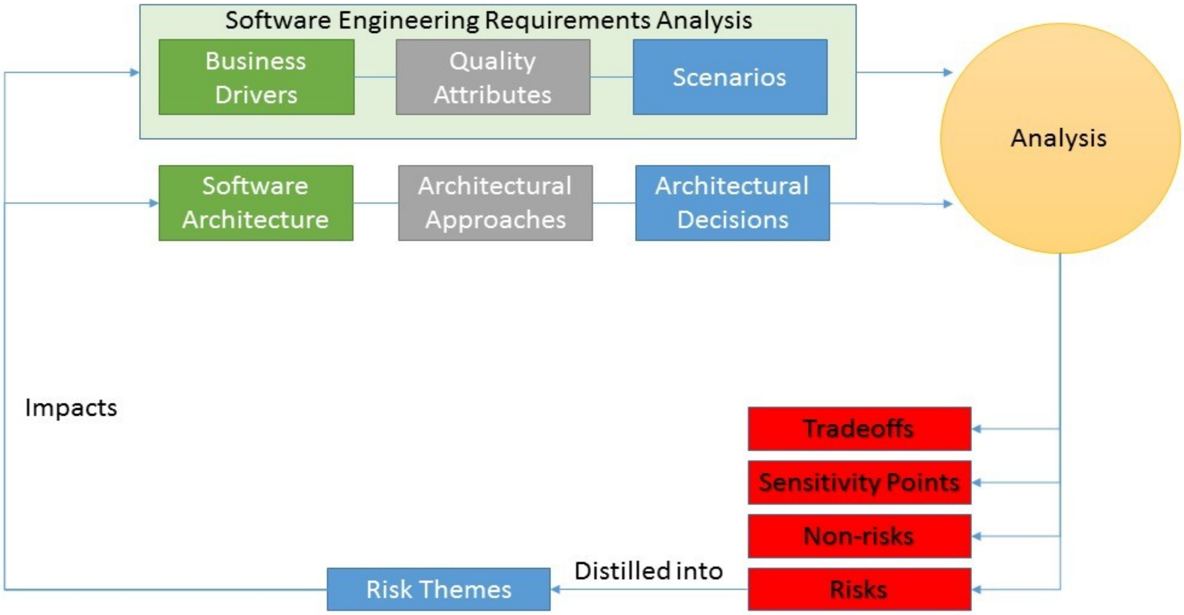


Figure 3.10: ATAM process.
Adapted from McGregor (2001)

3.13 Chapter Summary

Chapter 3 presented the research methodology followed in this software engineering project that targets to design and create a software architecture for online assessment systems. The Oates model (2006) was adopted to guide the project. Software architecture is a stakeholder-centred process, samples of stakeholders were drawn using purposeful and snowball sampling. The features required of the online assessment system were derived from the stakeholders. The features desired by each group of stakeholders in an online assessment system were incorporated into the design according to the Feature Driven Development (FDD) approach.

CHAPTER FOUR
DEVELOPMENT OF THE ARCHITECTURAL DEFINITION

4.1 Overview

This chapter submits and analyses the data collected using the methodology and tools detailed in Chapter Three. Chapter Four presents the findings and a proposed architectural definition for a software system that reduces impersonation in online assessments.

The chapter is comprised of the following sections; the research findings, the process of developing an architectural definition, a proposed architecture for an online assessment system and a chapter summary.

4.2 Research Findings

From the thematic analysis of the data collected from the interviews, focus groups and ATAM sessions, this research confirmed that impersonation is widely acknowledged as a threat by all education stakeholder groups. The faculty, quality, development and senior management groups admitted that impersonation in online assessments is a serious challenge that deserves closer attention and redress.

The thematic analysis provided information about the concerns of the stakeholders and the characteristics that stakeholders expect a quality and secure online assessment to deliver. The concerns of each stakeholder group are presented in Appendix A together with the interview questions that were used to solicit information from each stakeholder group.

These requirements were condensed and mapped into eight general categories. The analysis confirmed the assertions of McAllister and Watkins (2012), that there are certain conditions and requirements and critical expectations of the various stakeholder groups that must be satisfied as in an ideal assessment system.

According to McAllister and Watkins (2012), the conditions, expectations and requirements for an ideal formal assessment system are the identification of student (at start of assessment), authentication of student identity (at start of assessment), authentication of student identity (during the assessment) – presence verification, identification of student (at the completion of assessment), authentication of student identity (at completion of assessment), cost effectiveness, the students' experience and the likelihood of authentication success. These guided the qualitative determination of system effectiveness.

With reference to these conditions, expectation and requirements, this research measured the extent to which assessment systems meet these conditions using a scale of 0 to 10 for each condition (Preston & Colman, 2000)**.**

A *0 score* means the complete absence or failure to meet the requirement and *10* for the complete, perfect satisfaction of the requirement (Preston & Colman, 2000). The views of the stakeholders in the extent to which each condition is met by an assessment system were averaged to give the scores between these two extremes. Using this scheme, the "ideal" online assessment would yield a performance shown in Figure 4.1.

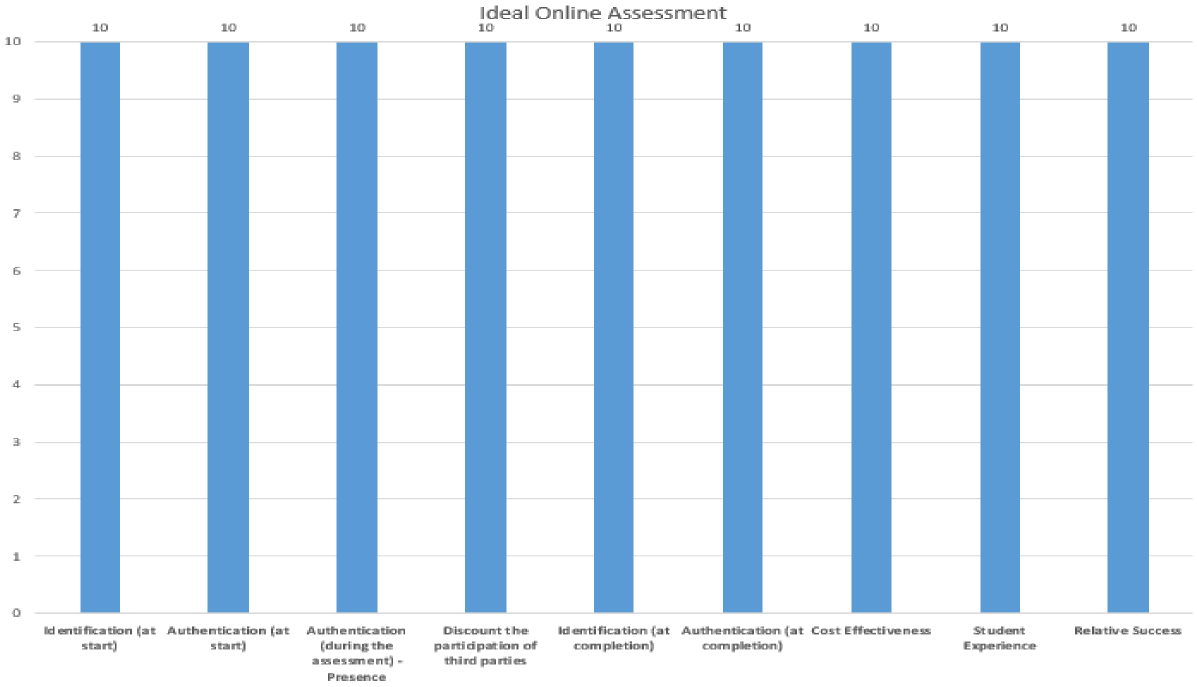


Figure 4.1: Performance of the ideal online assessment system

The stakeholders interviewed considered an "ideal" online assessment system as one that has the capacity to identify and authenticate the student at the beginning of the assessment session. It should also continually authenticate the student throughout the assessment. This means that the authentication of the student is expected to continue to include the procedures that mark the conclusion or submission of the finished assessment, discounting the involvement of third parties in the entire assessment session. This confirms the findings of Bedford et al. (2011) and Dunn, Meine and McCarley (2010).

All stakeholders emphasized the importance of the entire online assessment process being affordable and not cause excessive disturbance to the student's educational experience, concentration or comfort. Such an online assessment system is idealistic and would be fool proof to the academic offence of impersonation (Kirkpatrick, 2015; Rodchua et al., 2011).

4.2.1 The measures used to counter impersonation in online assessments

This subsection takes into account the research sub question 1 and sub question 2 posed in Section 1.6.1 and reports the findings.

SQ1: What measures do current online assessment systems implement to counter impersonation?

Online assessments are currently conducted in three basic ways i.e. remote non-invigilated assessments, centralized or venue-based invigilated assessments (Draaijer & Somers, 2017; Chuang et al., 2017) and online invigilated assessments (Anderson & Gades, 2017).

Different security mechanisms are employed in each of these different assessment situations to guard against impersonation. The following subsections discuss the measures that are instituted in each of these assessment situations.

4.2.1.1 Remote non-invigilated online assessment

This research found that this method is weak against impersonation. This shortcoming stems from the fact that it cannot discount the participation of third parties including the parents and peers in the assessment. Remote non-invigilated online assessments are commonly used for low stake formative progress and diagnostic assessments and can take place from any location and at any time chosen by the student within the time window set by then institution (Fask et al., 2014).

In this assessment method, the student uses a designated username plus password combination to log on to the Learning Management System and access the assessment. Once the student has logged in, the assessment proceeds and no further checks on identity or authentication of the student take place. Remote non-invigilated online assessment systems therefore offer no safeguards against impersonation after login (Bedford et al., 2011; Dunn et al., 2010).

All information that flows from the student's computer is considered as the work of the student associated with the captured username (Hollister & Berenson, 2009). The student however is expected to meet the costs of accessing and using Internet services. Despite calling upon the student to meet the telecommunication costs, this method of online assessment is considered economic for some students as the method does not force the student to forego other activity and travel to a specific place (Bedford et al., 2011).

4.2.1.2 Centralized / physically invigilated online assessment

The centralized, invigilated online assessments take place at a designated assessment center and at a preset time for the student or cohort of students under human invigilation (Fask et al., 2014; Hollister and Berenson, 2009). Figure 4.4 depicts a centralized, physically invigilated online assessment.

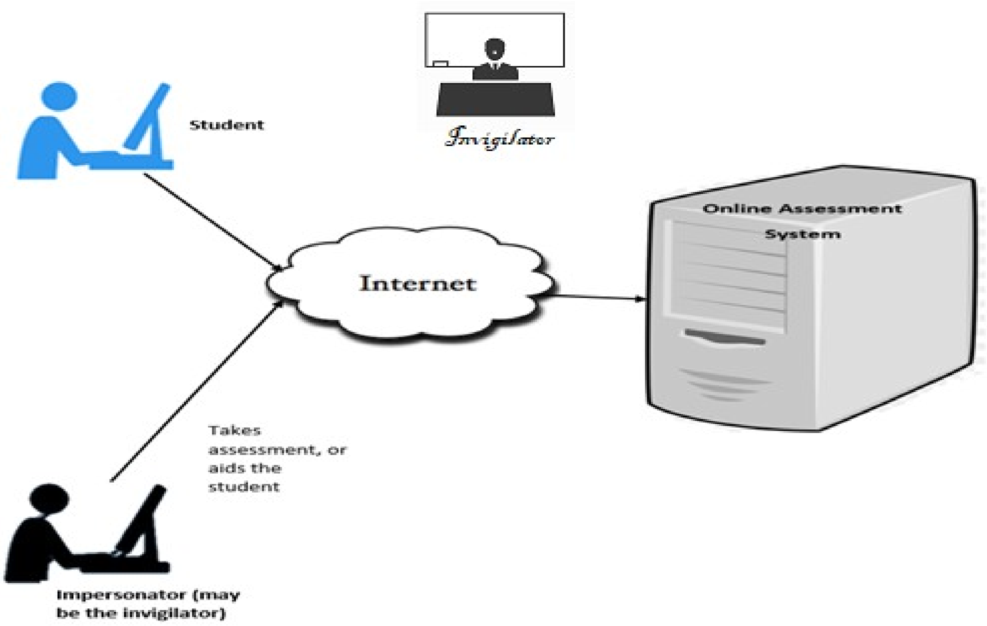

Student
Invigilator
Online Assessment System
Internet
Takes assessment, or aids the student
Impersonator (may be the invigilator)

Figure 4.4: Physically Invigilated online assessment

Through direct observation, this study found that before the assessment starts, the student presents some official proof of identification to the invigilator who may be a member of faculty and thus has a level of familiarity with the students. This familiarity provides the assessment method with some first line defense against the participation of third parties in the assessment (Kirkpatrick, 2015).

After the student has presented the identification document to the official and the identification is accepted, the student is assigned a device that is owned by the institution for use during the assessment (Mellar et al, 2018). The authors emphasise that the physically invigilated online assessment method assumes the legitimacy of the identification produced by the student i.e. the student brings their correct identity and the assessment official vigilantly validates all submitted identification. The physically invigilated online assessment system requires the invigilator to ensure that the student keeps the assigned workplace throughout the assessment and abides by the rules of assessment applied in the institution (Owusu-Boampong & Holmberg, 2015).

Some institutions place the student's computer system on lockdown, blocking access to other applications or websites during the assessment (Marsh, 2017). The study found that the use of other devices such as mobile phones and calculators are prohibited in the assessment venues and that invigilators could move around inspecting students at work. In other systems, the invigilators may have access to the student's desktop (Mellar et al., 2018). At the end of the assessment, the invigilator ensures that the students submit whatever work they would have done and sign off the system. This protocol aligns well with the online assessment system described in Fask et al. (2014) and Owusu-Boampong & Holmberg (2015).

4.2.1.3 Online invigilated online assessment

Online invigilation refers to invigilation of assessments over the internet through a webcam and other hardware such as microphones that capture live video for immediate viewing by the invigilator or record it for review (Foster & Layman, 2013). A range of commercial products are available for online invigilation e.g. Kryterion™, Software Secure™ and ProctorU™. The literature review gave the researcher insight into online invigilation systems (Table 2.1). These were discussed with faculty, quality managers and policy makers. The discussion showed that online invigilated assessments were being seriously considered by these stakeholders as a viable and feasible solution to some impersonation challenges.

4.2.2 Evaluation of existing online assessment methods in reducing impersonation

This Section presence the findings aligned to the performance of the discussed online assessment methods. The Section aims to answer the second research sub-question:

SQ2: To what extent are the current online assessment systems succeeding in countering impersonation?

This research showed that with regards impersonation, the security of the assessment methods discussed in Section 4.2.1 varied.

4.2.2.1 Remote non-invigilated online assessments

The effectiveness of the remote non-invigilated methods is affected by the ethical responsibility of the student as the method itself provides no inbuilt defence against collusion and impersonation. This makes the remote non-invigilated online assessments system vulnerable to Types B, C and D impersonation (Apampa et al., 2010).

This study learnt that the students and parent stakeholders favoured remote non-invigilated assessments because this assessment method affords the student the opportunity to take the assessment in the comfort of their home. The parents indicated that this enables students to take the assessment in an environment free from the “sceptical attention of distrusting and intimidating” invigilators and allowed the student to take assessments when they felt most prepared. Figure 4.2 portrays remote non-invigilated online assessments and how Type B impersonation can affect the assessment.

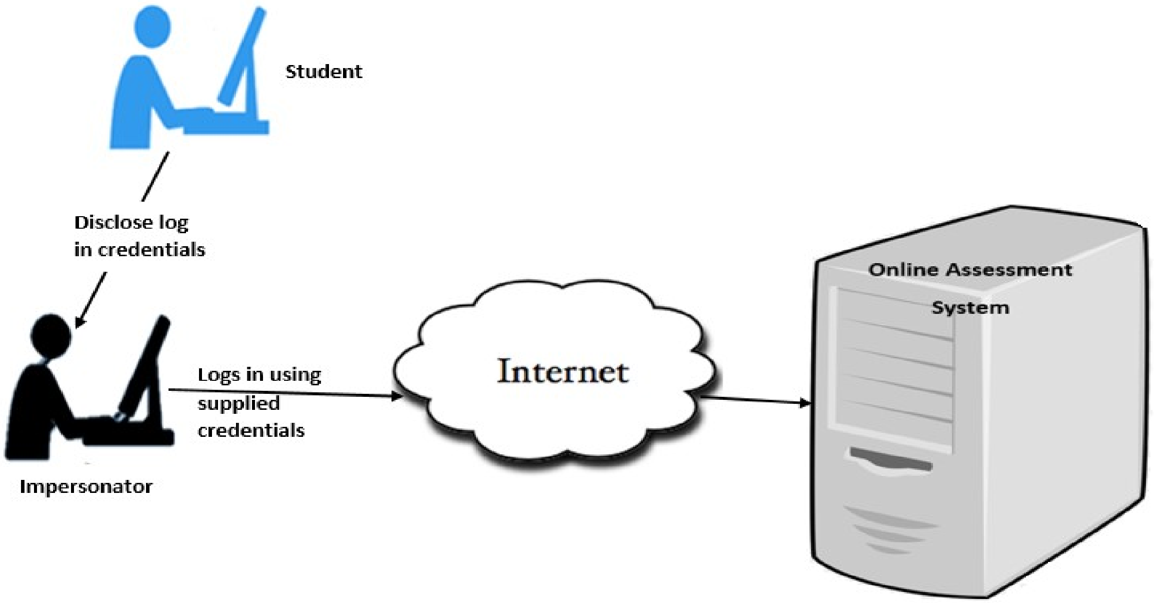

Student
Disclose log in credentials
Impersonator
Logs in using supplied credentials
Internet
Online Assessment System

Figure 4.2: Online non-invigilated assessment and Type B impersonation

Figure 4.3 is a summary of the performance of remote non-invigilated online assessments taking impersonation into account. According to information systems and quality management stakeholders, online non-invigilated assessments have a projected 50% success rate against impersonation as they have a strong reliance on the honour and ethical character of the student.

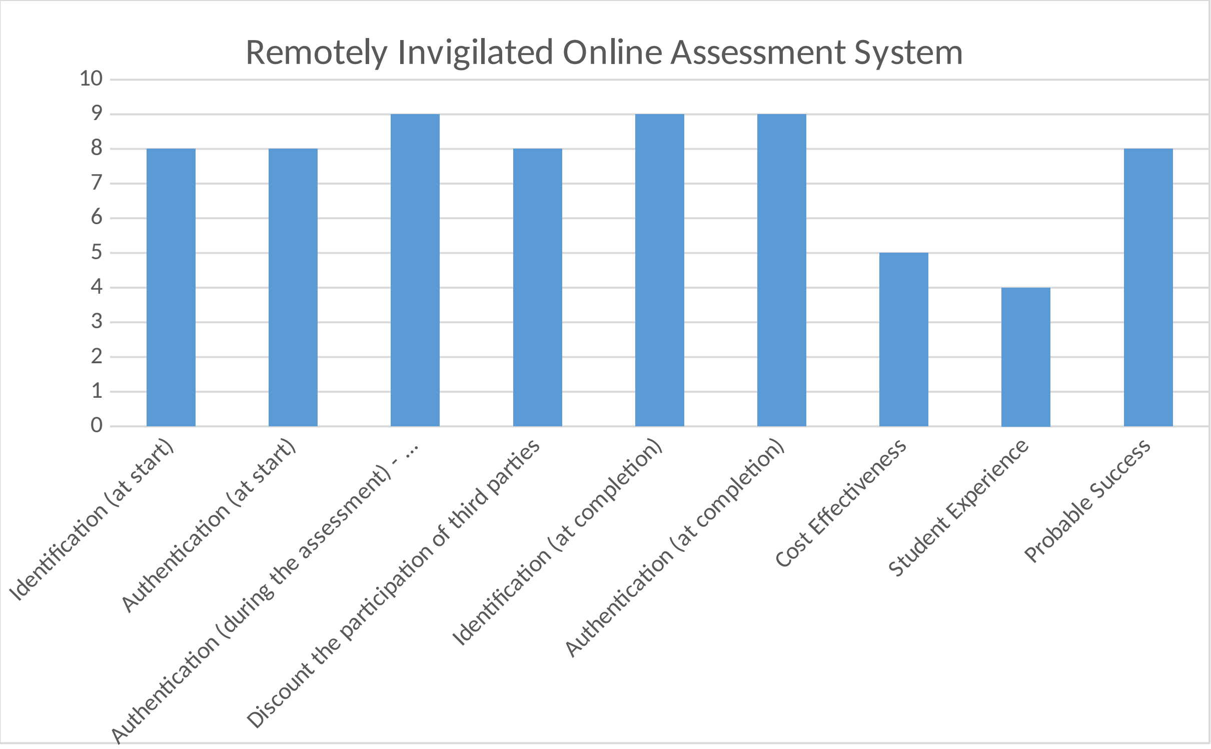


Figure 4.3: Performance of online non-invigilated assessment system

Taking the performance of existing online assessment systems that fight impersonation into account, this project proposes a software architecture solution to address the challenge of impersonation in online assessments. This solution is a product of the design and create research methodology that follows the Oates (2006) model.

4.2.2.2 Centralized / Physically-invigilated online assessments

The information obtained from faculty and quality management confirmed the findings of earlier research that against impersonation, physical human invigilation of online assessments falls short for various reasons. As posited by Foster and Layman (2013), the engagemnet of invigilators from within the institution weakens the security of the system as the invigilators themselves may have a stake in the outcome of the assessment and are familiar with the student. Foster and Layman (2013) argue that this may lead the invigilator to be less strict, deliberately or other wise, making human invigilation of online assessments vulnerable to Type A impersonation.

Fask et al. (2014) concludes that familiarity between parties present in the assessment venue, may lead to corruption or relaxation of some controls and routines e.g. the invigilator allowing content from other persons to become part of the student's final submission.

Physical invigilation of assessment suffers from other weaknesses that may beat even faculty invigilators e.g. similarities in facial features e.g. identical twins can substitute each other and have the smarter twin taking assessments (Ketab, 2017). According to Ketab (2017), the biggest weakness of the system lies in the invigilator deliberately assisting the student to beat the controls or complete the assessment. This reduces the probabilty of the method succeeding against impersonation. Engaging external invigilators also presents the challenge that impostors may succeed in impersonating the actual student e.g. lookalikes and doctored identification documents such as institution-issued identity cards (Ketab, 2017).

Physically invigilated online assessments can be more cost effective when the institution hosts assessments on local servers and deliver them to the students via a local area network or intranet, thus eliminating internet related overheads (Hollister & Berenson, 2009). The method can be considered expensive because it demands the configuration of a suitable venue for the assessment, designation of paid personnel to invigilate, requires the invigilator and the student to travel to a common assessment centre and demands usable infrastructure from the institution (Draaijer & Somers., 2017). The authors argue that such issues make the method expensive and take away the freedom of choosing the time and place where the student can take the assessment.

As Figure 4.5 shows, these issues make the human invigilation of online assessment method not so cost effective and hence a score that is less than perfect in the fight against impersonation. The stakeholders involved in this study agreed in giving a score of 90% to this method in meeting the requirements of the ideal online assessment system, despite the method having routines for authentication at the start of the assessment, during the assessment and at completion of the assessment.

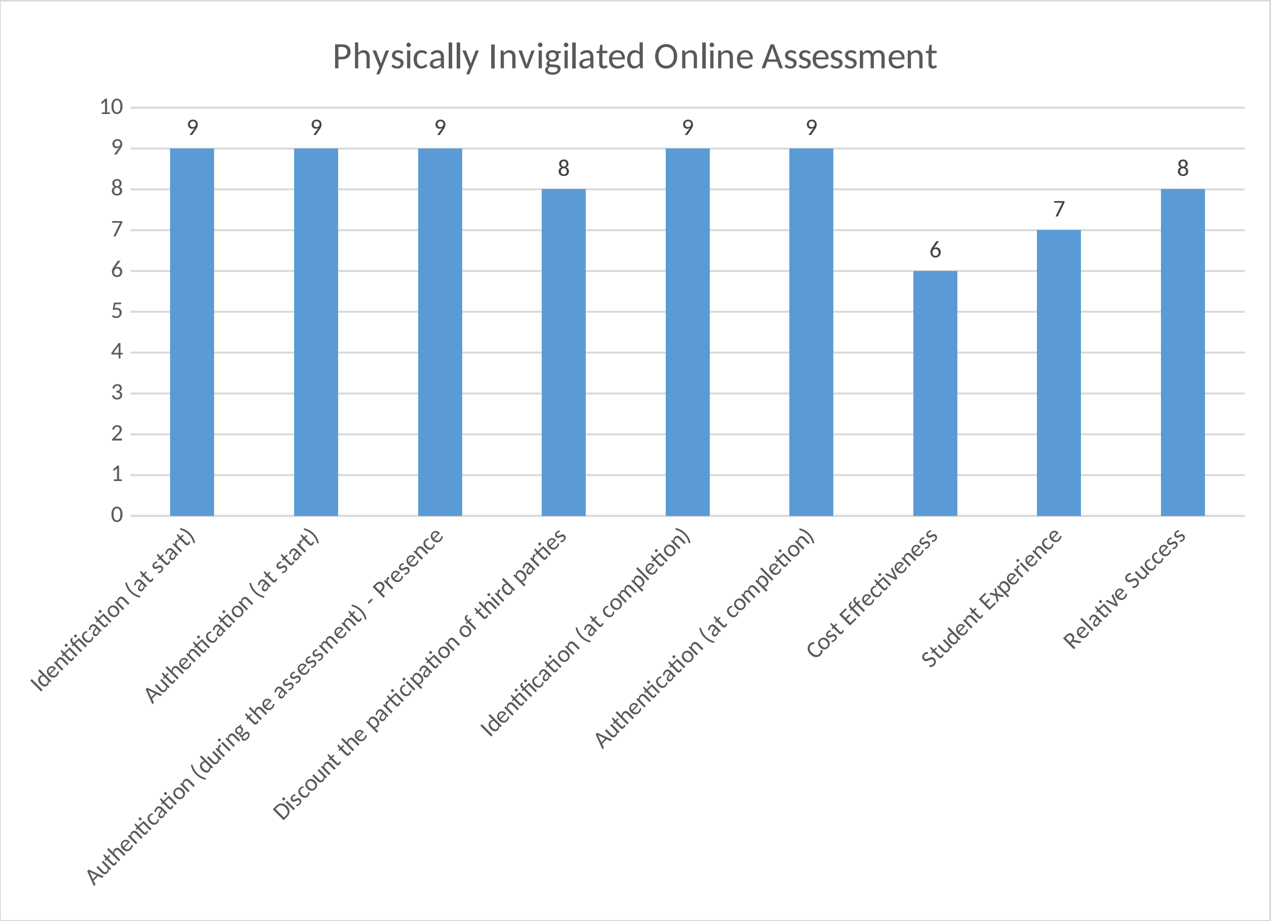


Figure 4.5: Performance of physically invigilated online assessment system

4.2.2.3 Online-invigilated online assessments

The literature review and the discussions with stakeholders showed that online invigilated assessment systems had potential to reduce Type B and Type C impersonation relatively well. The online invigilated online assessment is modelled in Figure 4.6.

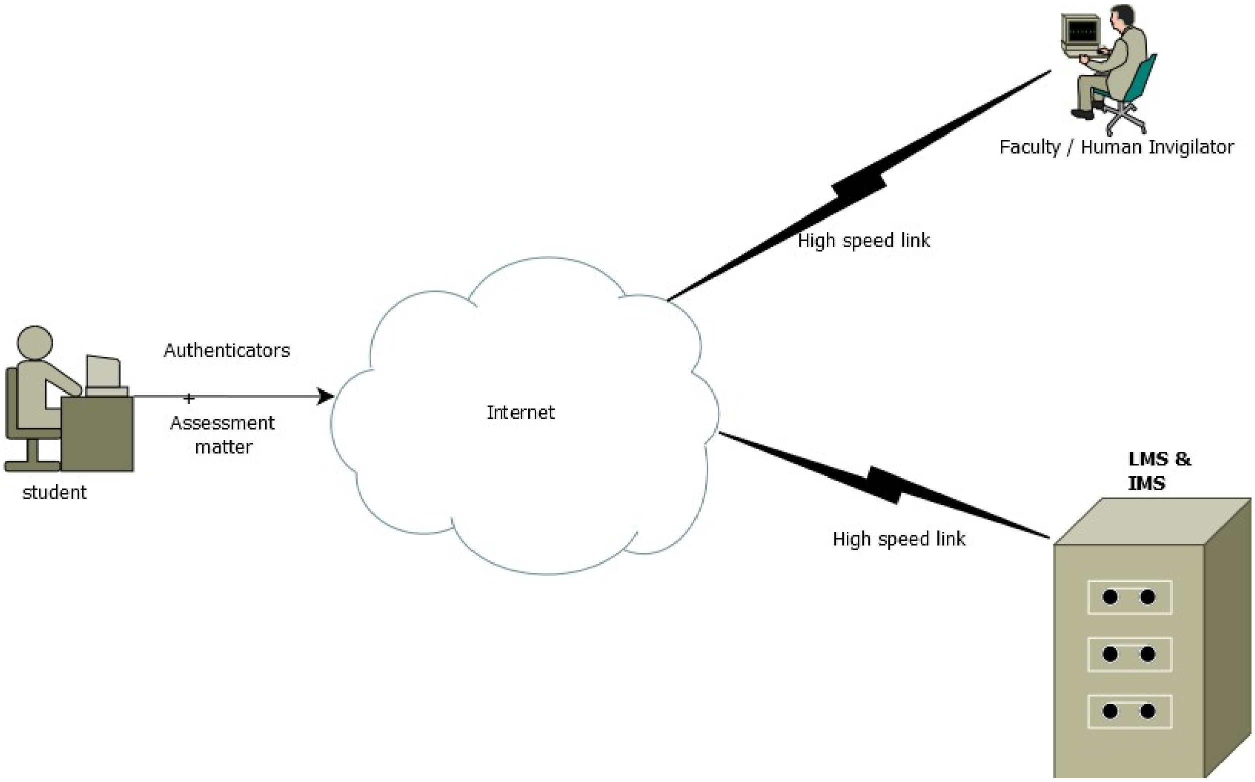


Figure 4.6: Online invigilated online assessment

Online invigilated assessment was not used at the institutions involved in this study. The option was mentioned and discussed at length with the faculty, technical and policy making groups. The discussion took into account the potential benefits of the technology and the potential challenges associated with it, in particular, the potential threats to privacy and confidentiality, intrusive nature of the invigilation process and cost implications (Hayton et al., 2018). This project's stakeholders projected that online invigilation of online assessments fairs as shown in Figure 4.7 with an estimated success of 80%.

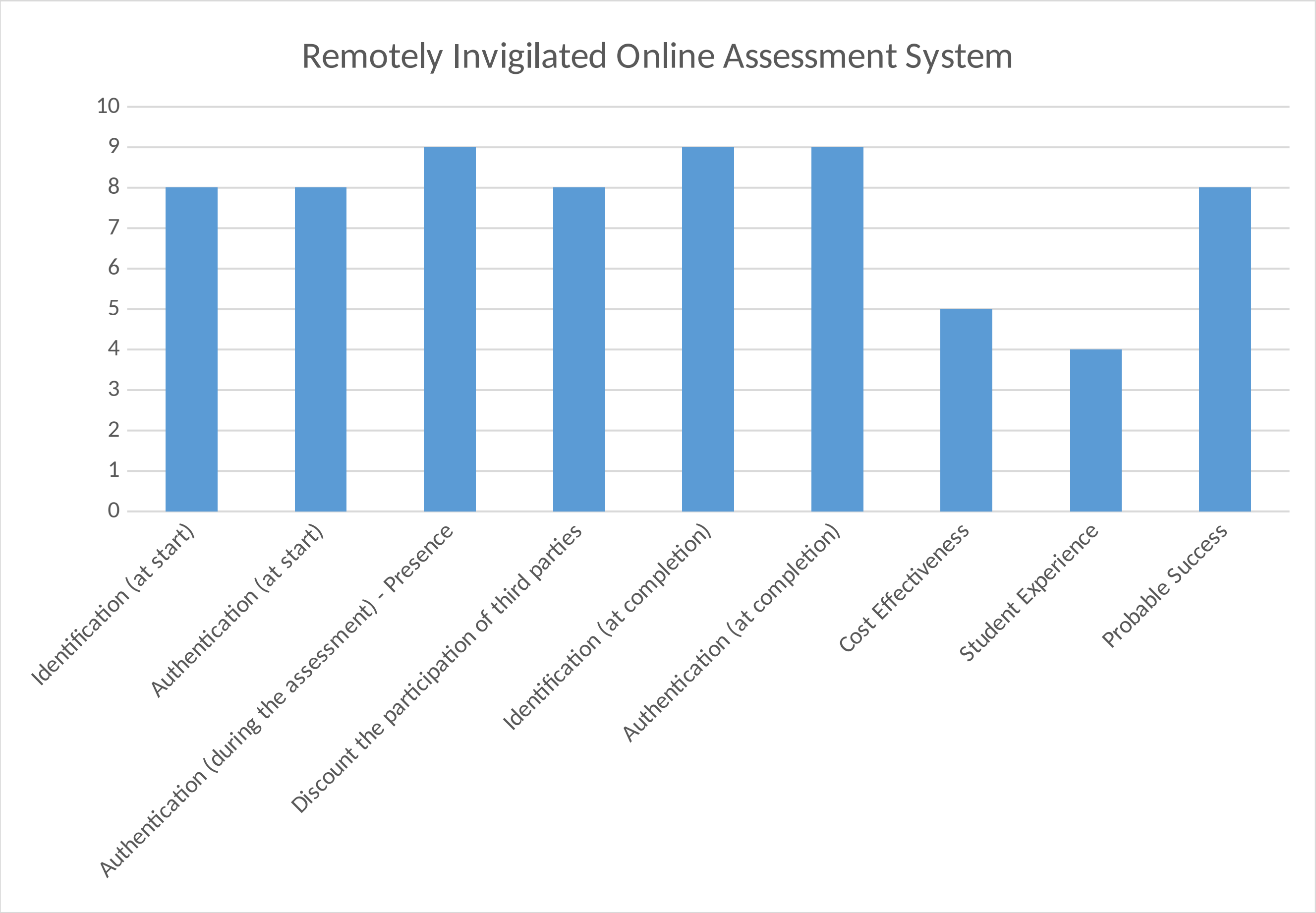


Figure 4.7: Performance of online invigilated online assessment system

4.3 The process of developing an architectural definition

The development of an architectural definition is a stakeholder centred process (Bass et al., 2013). As stated in chapter 3, the software architecture definition process is iterative, and aims to produce an architectural definition that adequately services the needs of its users.

The research project targets to deliver an architectural definition that is stakeholder-centred, structured, technology neutral, economic, scalable and flexible. Such an undertaking demands effective communication and understanding of the needs and concerns of various stakeholders (Ketab, 2017).

In this project, the development of an architectural definition is undertaken with the specific aim of soliciting and delivering the features revealed in response to the third sub question of the project:

SQ3: What features should a software architecture define in order to counter impersonation in an online assessment software system?

Stakeholders and their interests or concerns play a central role in the definition, design and documentation of software architectures. The concerns and interests of the stakeholders have a huge bearing on the design, acceptability and operation of the system.

According to Bass et al. (2013), the process of defining a software architecture involves a set of eight steps. The steps are identifying and engaging stakeholders, consolidate inputs, identify stakeholder scenarios, identify applicable architectural styles, produce a candidate architecture, explore architectural options, evaluate architecture with stakeholders and rework architecture, or refine the requirements.

The steps that make up the architecture definition process is shown in Figure 4.8.

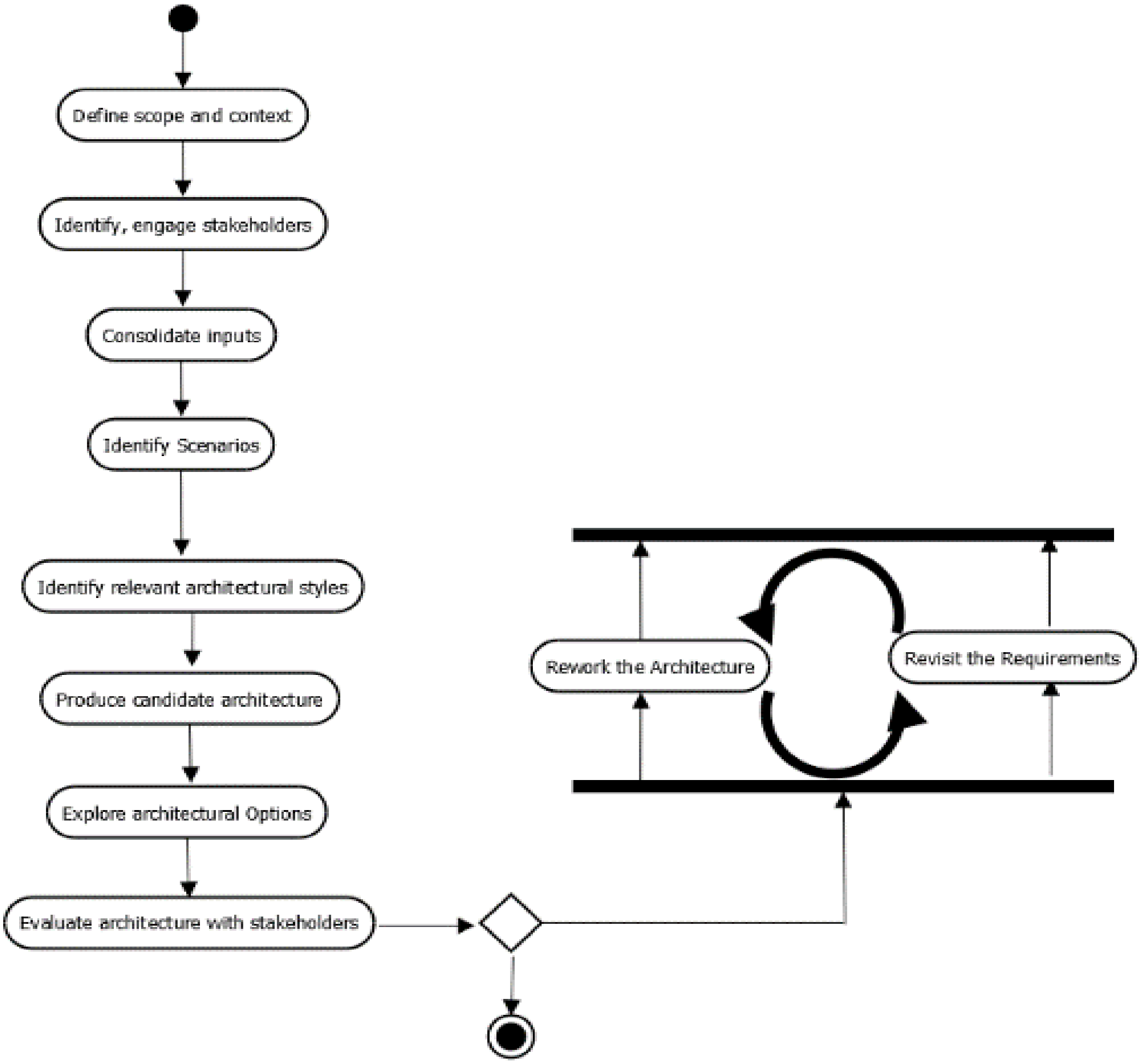

Define scope and context
Identify, engage stakeholders
Consolidate inputs
Identify Scenarios
Identify relevant architectural styles
Produce candidate architecture
Explore architectural Options
Evaluate architecture with stakeholders
Rework the Architecture
Revisit the Requirements

Figure 4.8: Architecture definition process

(Adapted from Bass et al., 2013)

4.3.1 Stakeholder identification and classification

As elaborated by Gama, (2017), this step aims to identify the system's key stakeholders, engage the stakeholders in the project and create a working relationship with them. This project's stakeholders are students, parents, educators or faculty who are also assessors and invigilators, curriculum developers. academic examination institutions and agencies, academic registrars, and system administrators. These stakeholders are described in Section 3.6.2.

4.3.2 Consolidate stakeholder concerns

Using the classification described Capilla et al., (2016) and the stakeholders presented in Section 3.7.2, stakeholder concerns were captured using verbal interviews in the form of individual interviews and focus group interviews. Stakeholder engagement provides a basis for understanding, validating and refining the initial concerns and expectations of the system.

Following the guidelines of Mann (2016), each stakeholder group that participated in the interviews was associated with a different theme and focus, related to their role and interests in the system. For each of the stakeholder groups, (described in Section 3.6.2), a different set of questions was posed in interviews to gather their concerns and interests.

The guidelines of Mann (2016) facilitated the processes of consolidation, prioritization and clarification of the stakeholder concerns (see Appendix A), to create a baseline of concerns for each stakeholder group. The process of consolidating stakeholder concerns served the secondary purpose of identifying and removing or reducing inconsistencies in the concerns expressed by different participants within the groups.

4.3.3 Identify scenarios

Appendix B presents the scenarios derived from the data collection activity involving stakeholders. These are depicted using Unified Modelling Language Use cases. According to Kruchten (1995), a scenario is a description of a situation that a system may encounter in its lifetime. Scenarios are used to assess the effectiveness or expected behaviour of a system design under a given situation. The activity of identifying scenarios aims to identify a finite set of scenarios that illustrate the stakeholder’s most important requirements. Scenarios can be designed to cater for both functional and non-functional requirements of a system (Lange et al.,2006).

The scenarios illuminate the key attributes required of the system and provide a basis of measuring the extent to which the system meets the concerns of the stakeholder (Hasselbring, 2018).

4.3.4 Identify relevant architectural styles

This step focuses on identifying the architectural style that can provide the best organization for the system. The main activity is to identify the architecture styles that are applicable and can address the concerns presented in the stakeholder scenarios (Hasselbring, 2018). Using tried and tested styles prevents the project from going off track and introducing unnecessary risks (Hasselbring, 2018).

4.3.5 Produce a candidate architecture

This activity aims to produce a basic draft architecture for the system. According to Laplante (2017), the basic architecture must reflect the concerns of the stakeholders and provide a basis for further evaluation and refinement of the architecture. The consolidated inputs from the stakeholders, architectural styles, viewpoints, and perspectives interact and guide the production of a draft architecture; which often shows gaps, inconsistencies or errors that need to be ironed out to improve the architecture (Mead et al., 2018).

For ease of presentation, this thesis uses the 4 + 1 “generic” design notation (Laplante, 2017) to document the software intensive online assessment system’s architecture through multiple, concurrent views.

The 4 + 1 model, shown in Figure 4.9, depicts the architecture of a software system as an amalgamation of the stakeholders’ viewpoints as the ways users, developers; management and engineers perceive the system (Lange et al., 2006).

Appendix C gives the candidate architecture using the Rational Unified Process (RUP) and the Unified Modelling language (UML). The 4 + 1 views clarified by Laplante (2017) for the candidate software architecture are delivered using the UML.

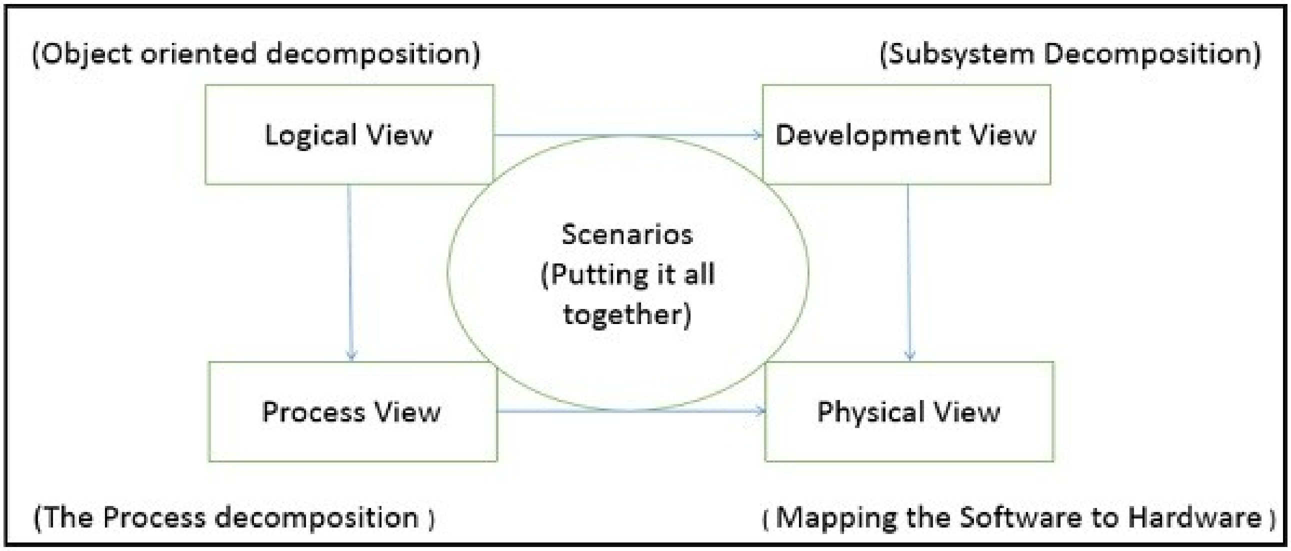

(Object oriented decomposition)
(Subsystem Decomposition)
Logical View
Development View
Scenarios (Putting it all together)
Process View
Physical View
(The Process decomposition)
(Mapping the Software to Hardware)

Figure 4.9: 4 + 1 View of architecture
(Laplante, 2017)

The four viewpoints that comprise the 4 + 1 model as described by Laplante (2017) are the logical view, development view, process view, physical view and scenarios / use cases.

1) Logical view

The Logical View is concerned with the functionality provided by the system namely, the system, as in the eyes of the end-users. Documentation tools that relay the logical view include class diagrams, use case diagrams, interaction diagrams and state diagrams.

2) Development View

The Development View details the system from a technical view i.e. as it is seen by programmers, software managers and technicians. The component and package diagrams serve the deployment view very well.

3) Process View

The Process View presents the dynamic aspects of the system and provides detailed explanations of the system processes, the components involved, the concurrency and synchronization of processes, performance and scalability issues (Kruchten et al., 2009). The process view focuses on the runtime behaviour of the system. The activity diagram and the sequence diagram are good illustrators of the process view.

4) Physical View

The Physical View is a representation of the non-functional, physical topology and interconnections of the software components of the system Laplante (2017). This view shows how engineers and other technical persons perceive the system. The deployment diagram shows the physical view in good detail.

5) Scenarios / Use cases

Scenarios / use cases make up the fifth view which is annotated as the "+1". These scenarios describe the interactions between object and processes in the system (Capilla et al., 2016). The scenarios or use cases serve to illustrate elements of the system, test, and validate the architectural design.

4.3.6 Explore architectural options

This activity targets to refine the system architecture, remove inconsistencies, identify and lower risks in the candidate architecture by exploring various architectural possibilities and taking objective decisions on which options to adapt (Capilla et al., 2016). The consolidated inputs, architectural scenarios, viewpoints, and perspectives amassed in the process thus far, are used to create a detailed and more accurate set of architectural views (Mead et al., 2018). This was achieved by testing the draft architecture using the scenarios created and described in Section 4.3.3.

Testing the draft architecture using scenarios clarified the software's potential benefits and demonstrates the extent to which the architecture is workable, meets the requirements of the stakeholders and exposes hidden weaknesses, risks and contradictions. This activity targets to isolate the best model for implementation as the solution architecture Laplante (2017).

This research proposes the integration of the Identification Management System (IMS) that authenticates users and the Learning Management System (LMS). This LMS provides content and assessments in an online environment (Narayanan et al., 2017) and the IMS provides a secure online assessment environment.

In the proposed architecture, the IMS sits directly "in front of" and "around" the LMS so that all connections to the LMS are authorized by the IMS. By following the proposals of Huffmeyer et al. (2018), this means that the identity management system will serve as a filter in the overarching Learning Management System to which it will pipe authorizations.

As an assessment takes place, the LMS and the IMS regularly exchange authentication data to provide continuous authentication and verification of presence as defined by Apampa (2010) and Gathuri (2014). Figure C3 in Appendix C, shows a class diagram for this architecture. The online assessment hosted by the LMS, continually messages the Identity Management System; feeding behavioural biometric data to facilitate continuous authentication that the authorized user is online (Lee et al., 2019), using the Internet connection to link the computer of the user with the LMS.

4.3.7 Evaluate the architecture with the stakeholders

Bass et al. (2013) posits that the selected architecture must be tested with the involvement of key stakeholders, to capture any shortcomings and gain their acceptance of the architecture. The research highlights that techniques such as the Architectural Trade-off Analysis Method (ATAM) facilitate effective evaluation of architectures in the face of potentially conflicting concerns and priorities. The evaluation activity aims at achieving consensus among stakeholders on the suitability of an architecture in meeting their consolidated concerns. Any required improvements and enhancements are captured and used in the next iteration of architectural design, as the project moves closer and closer to delivering a solution that best serves the stakeholder community.

4.3.8 Rework the architecture

According to Capilla et al. (2016), this activity aims to address the concerns that surfaced during the evaluation activities, by producing a new revised architectural design that better meets the objectives of the project expressed, in terms of stakeholder concerns. Techniques such as functional analysis and prototyping are used to rework or tweak the model in cycles that involve stakeholder (re) inspection. In reworking the architecture, a number of issues often undergo review. For example, the requirements may be revisited for clarity, (re) prioritization, changed or removed in light of time, cost and other constraints (Laplante, 2017). This activity often runs in collaboration and in-sync with exploring architectural options.

4.4 A proposed architecture definition for an online assessment system

Software architecture definition facilitates good communication and understanding between stakeholders leading to the production of a solution to a central or common set of problems (Capilla et al., 2016). According to the IEEE 1471 (2000), the architecture of a software system defines the elementary organization of a system embodied in its components and their inter-relations to each other, the environment, and the principles that guide its design and evolution.

4.4.1 Functional component description

Bass (2013) emphasizes software architecture as a combination of software elements, externally visible properties of the software elements and their inter-relationships. This proposed online assessment system, which comprises of these two high-level components is further documented in Appendix C.

The proposed architecture for a secure online assessment system comprise of the following six main components namely the student's computer, Internet access through Transmission Control Protocol /Internet Protocol (TCP/IP), cellular phone, Identity Management System(IMS), an Intervention Unit (IU) and the institution's Learning Management System (LMS).

The components of the proposed architecture play complementary roles in the assessment system as depicted in Figure 4.10 and explained below.

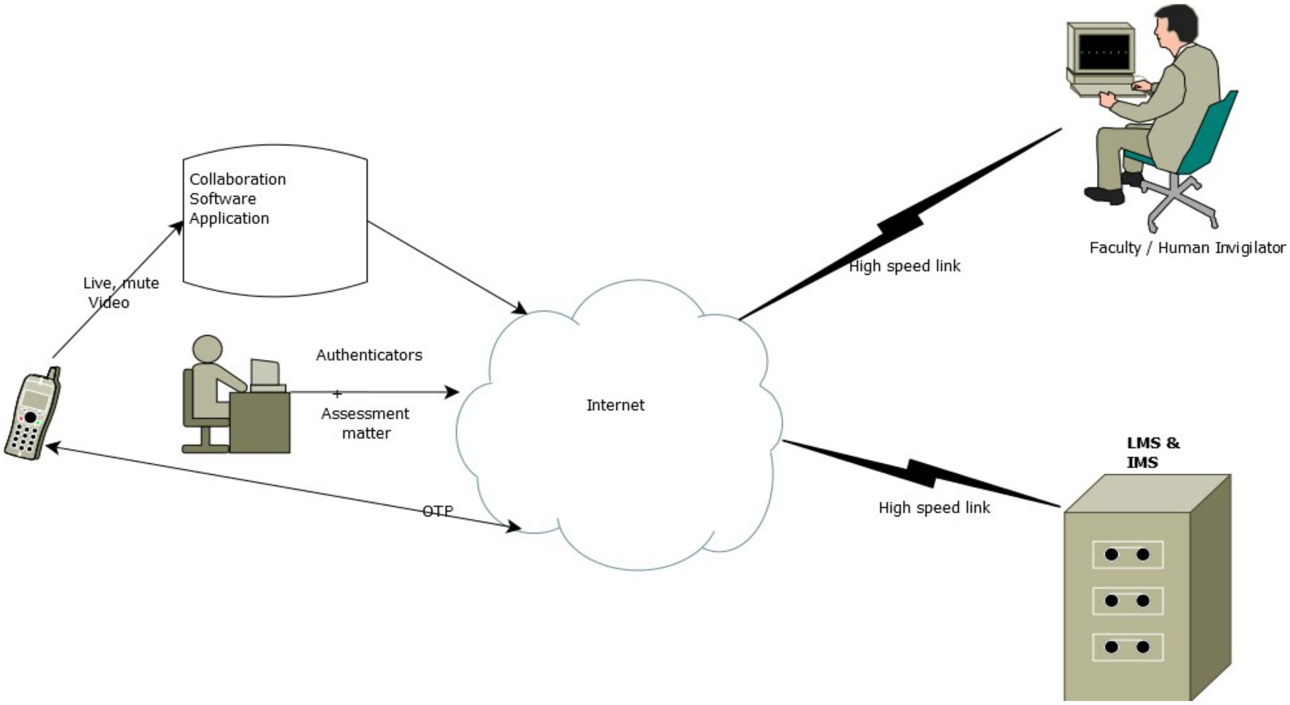

Collaboration Software Application
Live, mute Video
Authenticators + Assessment matter
OTP
Internet
High speed link
Faculty / Human Invigilator
High speed link
LMS & IMS

Figure 4.10: The proposed online assessment system in context

A. The *student computer*

In this architecture, the computer is the device that provides the student with the means to access and take the assessment through devices such as the keyboard and mouse (Alruwais et al., 2018). Other peripheral devices such as web cameras and microphones facilitate the capture of video, photographs and audio. The student's computer connects with the assessment system via an internet connection.

B. The *Internet*

According to Sun and Chen (2016), the Internet is the primary vehicle that transports traffic between the student's computer and the institution's information systems including the Learning Management System (LMS). The Network Interface Card (NIC) on the student's computer provides access to the Internet using the Transmission Control Protocol / Internet Protocol (TCP/ IP). The NIC provides a unique identity to the student's computer as the device used by the student throughout the assessment session (Shih, 2018). In the proposed architecture, this computer identity is combined with the student's identity details, such as student number or name to give each transmission of data a unique identity.

C. The *student cell phone*

This device is used as a token in the possession of the student as it uses the cellular phone number of the student that is officially registered as the contact number for the student. Through the General System of Mobile communication (GSM) and the Global Positioning System (GPS), the physical location of the cell phone and the student can be determined (Leng, 2018). The student's cell phone is used to send and receive One-Time Passwords (OTPs) which are used in student authentication at the start and conclusion of the assessment.

The cell phone further provides second channel streaming of events that happen in the student's environment through the built-in camera. The video stream feeds into a videoconferencing software system that feeds the session footage manager (Samangouei et al., 2015).

D. The *Identity Management System (IMS)*

The Identity Management System (IMS) monitors and manages all matters related to the identity and authentication of the student. The IMS targets to reduce impersonation by tracking the student's identity and variables within the environment in which the student takes the assessment.

The IMS comprises of a number of components or engines that perform functions such as student identification or recognition; persistently “listen” to activities happening in the LMS based assessment and keeps track of events that takes place in the student’s environment. For instance, the Identity Management System (IMS) has an engine for multifactor authentication. The engine requires the user to present a minimum of two factors for identification, from asset of factors such as passwords, one-time passwords (Grunin, Nassar & Nassar, 2019) and biometric authenticators such as facial recognition from different devices (Ligatti, Goldgod & Cetin, 2017).

At component level, the IMS is organized to function using pipe and filter (Wulf & Hasselbring, 2017), and event-based implicit invocation relationships (Lee et al., 2016) in order to provide these services at the beginning of the assessment and throughout the assessment. The multifactor authentication proposed in this research uses a multifactor authentication mechanism that includes username and passwords, geographical locators, possession of a one-time password capture cell phone (Grunin et al., 2019), challenge questions (Ullah et al., 2014), facial recognition, and other behavioural biometrics to identify and authenticate the student (Ligatti, Goldgod & Cetin, 2017).

The components of the IMS that achieve this multifactor authentication is described below:

i. To establish the identity of the student, the architecture utilizes a *Student Recognition Engine (SRE).* This engine incorporates challenge questions (Ullah et al., 2014) and biometrics such as still photography, facial recognition, video capture or recording, mouse mobility and keyboard dynamics. Machine learning authentication and these technologies inhibit third parties, including assessment officials, from impersonating the student through direct participation.

A *Multifactor Authentication Engine* (MAE) within the IMS couples with the assessment engine to provide the authentication when the assessment starts, and continuously throughout the assessment. A Multifactor Authentication Engine (MAE) is proposed to both deter and detect or report possible impersonation at all stages. The software architecture proposed for a secure online assessment uses a combination of authenticators (Ligatti et al., 2017). The authenticators fall in various groups such as knowledge-based authenticators, possession-based authenticators and biometric authenticators (Velasquez et al., 2018) at different times during the online learning and assessment cycle.

The MAE uses *Artificial Intelligence* (Omolara et al., 2019), in the form of a *Machine Learning Engine (MLE)* to capture, collate, compare and analyse online behavioural data such as typing characteristics (keypresses, latency between keypresses and typing speed) and mouse mobility (Adil et al., 2019).

This process makes the IMS learn characteristics about the student by collecting data that can be referenced for future authentication purposes.

ii. The *One-Time Password Manager* (OTPM) is a component of the IMS that can generate a unique string each time a student logs into the system and associates with the student and interactive session (Kishore et al., 2019).

iii. The OTPM works with the *Short Message System (SMS) Manager* to communicate with the student via short text messages on the registered cellular phone. The OTPM requires feedback to be within the restricted period (60 seconds) and works together with the *student location engine* and the *timer* (Wang et al., 2018).

iv. The *challenge question generator* is an algorithm that can read the student's biographical data and ask questions to the student (Ullah et al., 2014). Depending on the answers provided, the challenge question generator can set flags that can be used to grant to revoke access to the assessment system.

v. *The encryption kit* is a set of algorithms that provide security at the asset level on the user and other data processed in the system by converting data that traverses the network into a secure form that cannot be interpreted or used by external parties such as hackers (Le Saint et al., 2019).

vi. *The Student Location Engine* (SLE) is a mechanism that gathers details about the geographical location of the student by determining the location of the student's computer and cell phone. The SLE interrogates the Global Positioning System (GPS) to pinpoint the location of the equipment and the student (Pope and Gao, 2017).

vii. The MAE employs a *Machine Learning Engine (MLE)* to collect authentication data about the student and store these for retrieval when the student must be authenticated. Machine learning (Biggio & Roli, 2018) needs training upfront in order for it to be useful in the authentication of students. The MAE ensures that authentication happens each time the student accesses the online system, each session is monitored and a record of it is made in the student database by the Session *Footage Manager (SFM)*.

viii. The Session *Footage Manager (SFM)* can keep a recording of each assessment session in various forms that can be played back for example, an audio track, video stream, or clip sequence of still photographs. The SFM prepares data for forensics should a review of a session be required. The session footage manager also draws live feeds from the student's webcam (Ullah et al., 2014) and cell phone that is strategically placed to give a 360-degree view of the student under assessment to feed the faculty and artificial intelligence unit for online invigilation.

ix. The *audio-visual* manager is the component of the SFM that can capture data from the student's environment in the form of sound and visuals such as still photographs and videos (Bruno & Aparecido, 2009). This component feeds into the session footage manager and faculty videoconference visual display unit from the second channel video stream emanating from the student's camera phone.

x. The *Secure Facility Unit (SFU***)** is responsible for creating and maintaining a secure environment in which the assessment can take place. The SFU achieves this by quarantining the student computer and monitoring it to ensure that the student can make no external contact during an assessment. Student quarantine means that all extra ports on the student's computer are barred from use and no communication activity such as web browsing, screen sharing, printing or addition of new computer peripherals can take place during the assessment (Cartes et al., 2017). The SFU works together with the session footage manager and the audio-visual manager to ensure the security of the student's computer and environment.

xi. *The authorization engine* resides within the interface between the IMS and the LMS. The role of the authorization engine revolves around checking the status of control flags related to the assessment. When all flags are correct, the authorization engine issues a string to the LMS that allows the assessment to take place. The authorization flags signify conditions related to the student's identity, presence, location, and seclusion. These flags all help to ensure that the student assessment takes place under conditions that lend credence to the assessment event (Huffmeyer et al., 2018).

E. The *Intervention Unit (IU)*

The IU is a control component comprising of faculty members and artificial intelligence that provide a mechanism that keeps track of the rest of the online assessment systems including the

IMS and LMS components. The Intervention Unit has the capacity to step in, whenever any of the components such as the authorization engine returns a signal that calls for attention. For examples, when the student attempts to shut down the assessment before completion or the student goes "quiet" on all devices for an extended time period suggesting departure from the assessment environment. When more than one face is detected by the SRE or the second channel video stream, the IU would raise a flag for possible third party participation.

A flag would also be raised when the MLE reports a mismatch in the user's behaviour against the learned student behaviour (such as mouse dynamic behavioural biometrics). The A/V manager can raise a flag when a suspect video feed, still photo or audio (suspicious sound / voice is detected).

F. The *Learning Management System*

The Learning Management System (LMS) is the core component for the provision of educational services and products such as course materials, student-educator correspondence, student databases and assessments. It is the LMS, which also houses the students' database and the assessment system.

The student database is a secured central data repository within the institution that houses student data suitably organized for immediate direct access. The student database stores biographical student data such as names, date of births, addresses, secret questions and answers, the usernames and passwords and biometric data.

The *assessment system* is responsible for all transactions that relate to files and other objects that store questions, data and algorithms related to the actual online assessment. The core of the assessment system is the assessment engine, which contains the assessment *question bank*, a *randomizer and a timer.*

The *question bank* is a database comprised of questions and answers kept in a secure encrypted format. This must be large enough to allow the generation of a large number of unique assessments for students in real-time.

The *question randomizer* is an algorithm suite that generates different combinations and permutations from the structured question bank. The question bank is structured such that questions of the same level of difficulty are grouped into bands. The randomizer enables the creation and administration of unique, fair assessments for each student by systematically picking an equitable number of questions from each band in the question bank (Chua et al., 2019).

The *timer* is a clocking device that synchronizes all processes during an assessment session, defining start time, completion time, and placing bookmarks in the session, video or audio streams (Kanamarlapudi, Hsu and Ramalingham, 2016; Wang et al., 2018). The architecture of the proposed online assessment system is shown in figure 4.11.

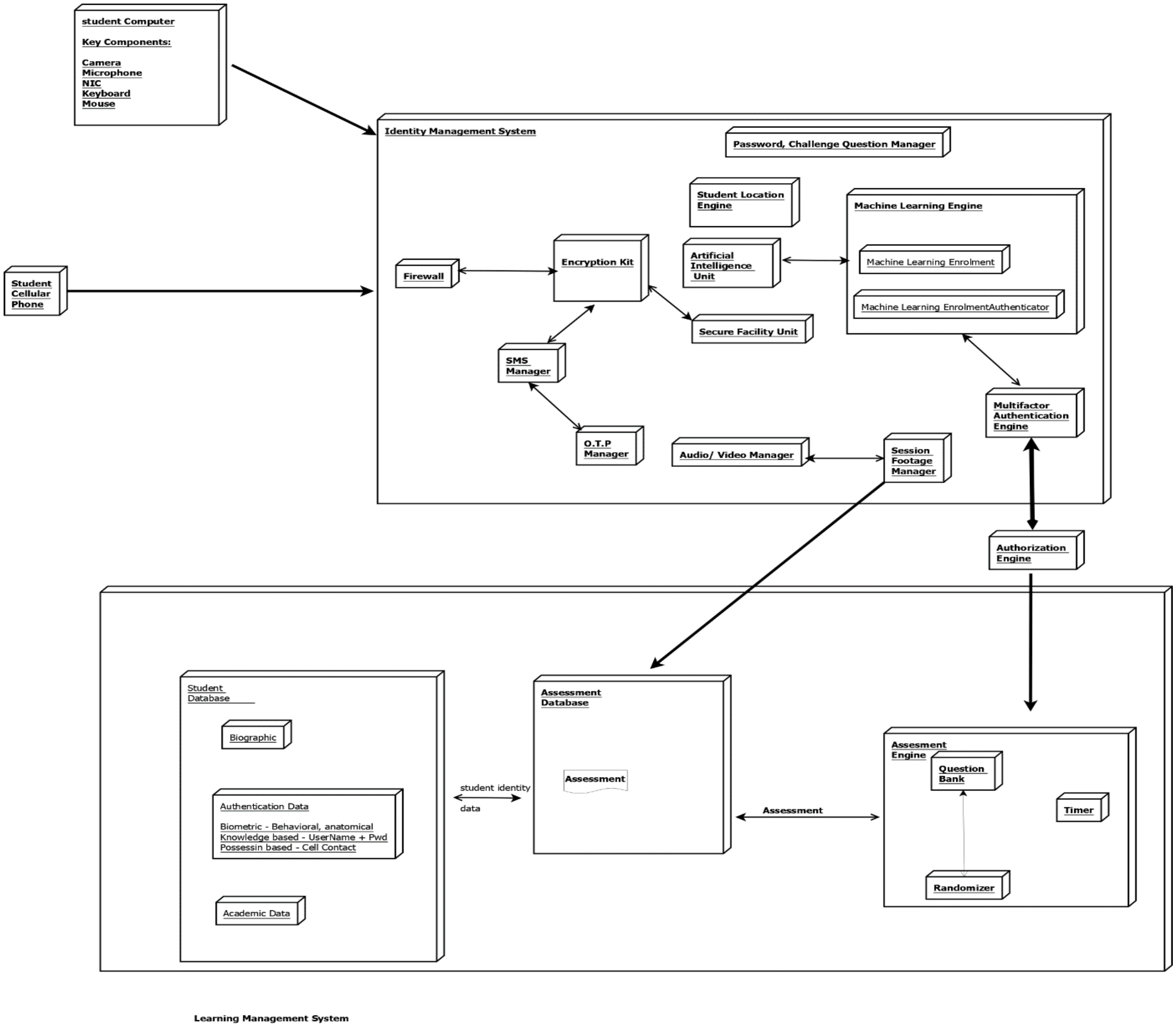


Figure 4.11: The architectural components

4.4.2 Process description

This section describes the processes that take place within the proposed system in three basic situations that the student typically can engage in with the online assessment system i.e. when the student enrols for the online course, when the student studies the course online and when the student takes the assessment.

The roles played by the components described in section 4.4.1 are further explained in the following processes.

4.4.2.1 Student enrolment onto the online eLearning system

For enhanced security and recovery purposes, account recovery information such as secret challenge questions and the secret answers must be captured (Ullah et al., 2014). When a student registers for a course, personal student data such as identification, contact address and phone number is captured into the students' database. A unique username such as student number or email address and a secret password are set.

These pieces of data are static as they generally do not change during the course of time. Basic biometric data, such as facial photograph, voice, fingerprint and so on may be captured and encrypted before they are stored as part of the student's record on a secured student's database Okada et al., (2019).

4.4.2.2 Student engagement using the eLearning system

The primary purpose of the student enrolment process is to create a baseline of the student's identification and distinguishing attributes within the system for future reference. During the term or semester, as the student engages in the course of study, the Identity Management System is trained using identity and authentication data about the student. The student engages with the system through a computer that has a microphone and camera enabled so that authentication routines can make use of them.

The aim of this specification is to cultivate acceptance and comfort with the security measures, simultaneously collecting student behavioural biometrics into the SRE and MAE. The collected data creates a unique baseline or *behavioural profile* for each student on the student database (Okada et al., 2019).

Each time the student engages in an online activity such as taking a quiz or other communication with the distant educators, the *Student Recognition Engine (SRE)* passively captures student identification information using the keyboard and mouse dynamics (Karim et al., 2017). Periodically, challenge questions are posed to the student to validate the contents of the database. This gives an online assessment system many opportunities to confirm and validate that the student is who they claim to be (Ullah et al., 2014).

4.4.2.3 Student engagement for assessments

This work proposes that before an assessment can take place, the online assessment system requires the following few pre-conditions to *first* be satisfied. The student must ensure that they take the assessment from a secure place where equipment and themselves will be safe and able to focus.

It is important for the student to have in their possession a functional cellular phone that connects directly to the computer e.g. via a USB port and is equipped with a functional camera. The phone must be adequately powered and reachable through the contact number listed in the student's record. It is important for the student to have a good quality Internet connection and a computer that has audio-video capability with a functional web camera and microphone / sound system.

The following steps are followed inside the proposed online assessment system:

a) When the student logs into the assessment system using the designated username and password, the Identity Management System (IMS) Multifactor authentication engine validates the name and password against entries kept on the student database.

b) When the IMS Multifactor authentication engine finds a match between the supplied username and password credentials and the database record, the system starts collecting behavioural data and gives the student access into the assessment system (Bowness, 2016).

c) The *One-Time Password Manager (OTPM)*, situated in the IMS generates a unique alphanumeric OTP string or a CAPTCHA (Agrawal et al., 2019). The *Short Message Service (SMS)* transmits the OTP or CAPTCHA to the student's registered cell phone number. On the computer screen prompt, the student should provide the OTP, CAPTCHA symbols within a stipulated short space of time (60 seconds) into the computer. The CAPTCHA may alternatively display on the computer monitor and the student requested to scan it with their cellular phone.

d) When the student captures the OTP or CAPTCHA and clicks the send option, the OTP/CAPTCHA manager matches the captured OTP or CAPTCHA entered by the student at the computer user interface with the OTP/CAPTCHA that was sent to the student's cellular phone.

The two strings must match in order for the student to proceed and access the system's resources (Agrawal et al., 2019). Correct OTP triggers the *Student Location Engine (SLE)* to triangulate the student's geographical location. The SLE extracts the location information from the Global Positioning System (GPS) provided, by pinging the cellular phone (Mahbub et al., 2016).

As the assessment process continues, the IMS periodically polls the student cellular phone for location data. This non-intrusive process provides a means of tracking the location of the mobile device against the IP address of the computer from which the assessment is taken. Next, the system reads the Internet Protocol (IP) address and *Network Internet Card* for the Media Access Control address off the computer system from which the student is sending data (Shih, 2018).

Incorrect OTP or CAPTCHA returns an error message to the student. If the OTP time of 60 seconds has not lapsed, the student can retry capturing the OTP. When this time period lapses, a record is made in the assessment system and a potential flag raised in the intervention unit for possible intrusion. The student will have to wait for some time before retrying to log on. The exact time period is set by the institution.

e) The IP address can be used to lookup information of the exact hardware (media access control address) of the student's computer as well as the location of the computer. The student's location is verified as the geographical position provided by the computer and cellular phone within a reasonable margin of error.

   A conflict in the location of the two devices at any time during the assessment, suggests that the registered cellular phone and the student computer are not in the same geographical location and thus a possible attempt to commit Type D impersonation (Apampa et al.,2010). A red flag is raised by the system and the assessment cannot proceed until the conflict is resolved, possibly with the involvement of faculty.

f) Successful login and location mapping initiate the *Secure Facility Unit* (SFU) to quarantine the student under assessment (Cartes, Frantz & Reed, 2017). The following steps describe how the proposed system achieves the quarantine:

i. *Lock the browser on the student computer* – This measure ensures that the student becomes unable to open online sources, other applications such as instant message software to reach out to external persons during the assessment.

ii. *Remotely block the computer's communication ports* – This guarantees that the student cannot share their screen with possible impersonators, colleagues or accomplices.

iii. *Disable print screen / shooting and clipboard facilities for copy / move and paste* on the screen and through the keyboard so that the student cannot take content from the assessment to other applications.

iv. These steps above effectively isolate or quarantine the student's computer and limits the computer's functions to those that are necessary for the assessment to take place.

The *Audio – Visual Manager* remotely activates the sound (audio) and picture and video hardware on the student's computer. This facilitates remote monitoring of the student's environment using inputs such as sound and visual (e.g. still photography or video).

g) The student is then asked to connect the cellular phone to the USB port and strategically position it to provide a good view of the student and the computer that they are using for assessment. The A/V manager configures the cellular phone to feed live video into the computer system via the USB port for transportation into the Artificial Intelligence unit and faculty videoconferencing system (Rao et al.,2011).

h) When the student's computer is secure and the A/V feed from the student's environment detected, the *Student Recognition Engine* takes over. The SRE serves to identify the person sitting in front of the computer, against the images on file for the registered student. The SRE uses recognition technology to determine the person seated in front of the computer. Recognition may employ different forms such as:

Still photography – The A/V manager captures still images of the computer user and relays the image to the SRE. The student recognizer uses facial recognition by scanning the student's images on the student's database. A successful search is when the face of the computer user at that time matches the face on the student database with the corresponding identifier e.g. student number and student name (Samangouei et al.,2015).

Challenge questions – A set of one or more questions are read from the logged in student profile and answers sourced from the user of the computer at that point in time. As this is a knowledge-based authenticator, the user must correctly answer the questions within a limited amount of time and within the constraint of a limited number of attempts (Ullah et al., 2014).

Audio / Voice recognition – The installation may prompt the student to verbally submit some evidence to support their claim to identity. This may be an answer to a challenge question, student number, or other phrase. This Student Recognition (SR) method that uses voice recognition attempts to match the voice fed into the audio capture device, against the voice samples that are kept as templates during the enrolment/registration process of the MLE (Rudrapal et al., 2012). The SR only permits the session to proceed when the person interacting with the computer is the registered student.

i) When the student has been recognized or authenticated, and before the actual assessment begins, the institution's code of honour is displayed on the student's interface. *The Code of Honour* targets to reinforce sound academic practices in students under assessment.

At the foot of the code of honour (Jones, 2009), the student is required to show that he / she has read the document by choosing an "*Accept"* option through an input device on the computer, such as a keyboard press or a mouse click. Upon acceptance of the code of honour, the *authorization engine* is triggered to generate an authorization token to the LMS.

The authorization token is a cryptic string that concatenates the following values into a single value that is made up of the following elements:

studentID = the identity of the student (email address or username)

locationID = GPS location of student

MobileDeviceID = the IMEI identification of the student's cell phone concatenated with registered cellular number

NIC/MAC = The Network Interface Card or Media Access Control Address of the student's computer

MLEFlag = the Boolean value signifying positive biometric identification of the student. This will switch state when a biometric test fails

SFUFlag = The student Facility Unit issues a flag signifying complete lockdown of student computer. If a lock fails for instance, communication ports not closed, this flag will show that status
AMFlag = A Boolean flag showing the readiness of the audio-visual state of the student's hardware
StudentRecFlag = a flag signifying that the student has been recognized.

j) The authorization token is relayed towards the Identity Management System / Learning Management System (LMS) interface regularly (Wang et al., 2018). The assessment session can halt or terminate should a condition be violated at the start or during the assessment by an incorrect read on any of these variables.

k) On receipt of the authorization token, the LMS assessment engine locates the assessments for which the student made bookings. The list of booked assessments is displayed to the student so that the student can select the ***one*** assessment to start.

l) In the assessment subsystem the question randomizer generates a unique assessment for the student by applying an algorithm to the banded question bank.

4.4.2.4 Continuous authentication during the assessment

In the proposed online assessment system, once the Identity Management System (IMS) has issued the authorization to start the assessment, the assessment can begin. The following processes characterize how an online assessment is started using the proposed architecture:

a) *The Timer* initializes and a running countdown clock displays on the student's interface. *The timer* listens to the *intervention unit* for significant events. Significant events are events that can arise during the assessment such as periods of inactivity, interventions from faculty, attempts to exit.

b) *The Multifactor Authentication Engine (MAE)* starts and continues to run for the duration of the assessment. The MAE continually listens to the assessment, tracking the trained student behavioural dynamics such as keyboard interaction and mouse mobility. Each time the student is successfully authenticated, the MAE reads the dynamic biometric and compares it with the stored biometric pattern for the student.

c) The timer synchronizes events in the entire assessment system, like the time used by the SLE, SRE are assessment time units. For instance, the 20th minute of assessment establishes a position of control, bookmark in videos, and the times when authorization strings are sent as the assessment proceeds in the presence of continuous assessment.

d) At random intervals the SLE, polls the student's cell phone to read the location of the device. The location of the device is compared against the established location from which the student is taking the assessment.

This means that for the assessment duration, the student's environment is monitored in a number of different ways.

Low latency video capture: Derived from the student's webcam and the second channel feed from the cell phone, this technology may be used to provide human invigilators with a live feed of the student taking the assessment.

Still photography: Periodically, and at random intervals, the SRE engages the A/V manager to capture still images of the student in assessment. The captured images are channelled to the SR engine for facial recognition of the computer user.

Audio monitoring: The environment in which the student is taking the assessment is monitored for sound, especially human voice and other such intrusion, or unauthorized assistance from any source.

Second channel video feed: The student's cell phone, strategically positioned, provides a continuous 360-degree video feed of the student's immediate environment, facilitating detection of other persons or objects in the student's environment. This live feed can be channelled to faculty for remote invigilation by a member of faculty who sees a window for each student in assessment, on one screen similar to videoconference displays presented by software products like Zoom™ and Microsoft Teams™.

The student provides answers online and algorithms in the encryption unit are invoked to immediately encrypt the answers. During the assessment, the assessment engine listens to the intervention unit, Machine Learning Engine (MLE), Secure Facility Unit (SFU), the Audio/Visual Manager and the Student Recognition Engine (SRE), which collect vital data such as the biometrics of the student, environmental events and location of the student.

Once encrypted, the bundle is channelled via the Internet towards the LMS. Each input stream from the user is a bundle that comprises the following blocks of authentication information - StudentId + locationID, MobileDeviceID, NIC/MACID, MLEFlag, SFUFlag, AMFlag, StudentRecFlag.

Every bundle of data from the student's side is validated using the initial values for each of the controlling variables used to detect or deter malpractice during the assessment.

The assessment engine only allows the assessment to continue when all the flags from the authenticating bundle are correct as defined for the accepted environment and conditions for assessment.

Whenever the assessment suffers an interruption or intervention, the Intervention Unit (IU) responds differently in different situations, for example when Biometrics fail, the IU can lock the assessment pending directive from the Faculty. The IU may trigger the MLE to recheck the student's activity when there is suspicious activity in the student environment. This would trigger the A/V to place a special bookmark at a certain point in the video for analysis after the assessment.

When any of these events happen, the OTP generator and the SLE are directed to confirm student presence and the location of the computer by sending, receiving and processing device identification and location information as described at the start of the assessment. The timer timestamps the interruption or intervention and instructs the *Question Randomizer* to bookmark the last question answered and regenerate the balance of the assessment. To complete the process, the student is prompted to answer a randomly picked challenge question.

For the record, all details about the interruption are captured and kept on record under supervision of the *Session Footage Manager (SFM)*. The SFM can facilitate video and audio playback of the assessment session and other recovery events, should the need arise. When the interruption is managed through faculty or artificial intelligence, intervention is complete. The intervention unit surrenders control back to the IMS and *assessment engine* so that the assessment can continue from the appropriate point, with the timer's countdown continuing.

4.4.2.5 Authentication at conclusion of the assessment

When the student finishes the assessment, a submit sequence begins to run in the proposed system. The sequence is described as follows:

1. When the student clicks the "submit" button on the computer, the One-Time Password Manager (OTPM) generates and sends a new submit OTP or CAPTCHA to the student cellular phone to confirm the intention to submit the assessment and sign off the assessment system.

2. The student returns the submit OTP or CAPTCHA and the GPS location of the cellular phone is used to determine the location from which the student sends the OTP or CAPTCHA.

3. Upon receipt by the OTPM, the submit OTP or CAPTCHA is validated.

4. The cellular phone's location is compared with the location of the computer from the NIC and IP address. If the two matches, the submit OTP is appended to the closing string for the session.

5. If a match is found:

    a. The Identity Management System (IMS) collects sign off audio and video data from the Audio-Video Manager (AVM) and appends it to the student's closing string.

    b. The Secure Location Engine (SLE) releases the student's computer by re-activating all blocked functionality.

    c. The A/V system is brought down.

    d. The student's system exits the assessment environment.

6. If any of the comparisons performed in this sequence of steps fail, an intervention flag is raised, and the intervention unit takes over to resolve the situation.

4.5 Fighting Impersonation using the proposed architecture

In chapter two, section 2.6, the ways in which impersonation can take place in assessments were explored. Drawing on the findings of Apampa et al., (2010), impersonation threats fall into four (4) broad categories as shown in Table 4.1 (Apampa et al., 2010; Gathuri et al., 2014; Sabbah et al., 2011).

Table 4.1: Impersonation threat types

Threat Type	Definition
A	In an invigilated assessment, either the invigilator does not notice the case of impersonation OR they notice it and do not act against it for reasons such as bribery, coercion or empathy. This is connived impersonation.
B	The legitimate student provides their security information to other parties who complete the assessment on their behalf purporting to be the holder of the identity given in the security information.
C	The legitimate student logs onto the assessment system and permits another third party to take the assessment on his or her behalf.
D	This happens when the legitimate student logs onto the assessment system and takes the assessment, working in a cohort with a third party.

To reduce the likelihood of impersonation, an assessment system should *guarantee fairness* to all assessment candidates (Sabbah et al., 2011). This means that the system must cater for the challenges of student malpractices such as unfair retaking of assessments, obtaining help from any unauthorized human or computer sources, and unauthorized collaboration with others on individual assessments (Rodchua et al., 2011).

The proposed software architecture uses a randomizer to fight off unfair retakes by delivering a unique assessment for each student assessment session. The assessment questions are derived from a sizeable, banded and balanced question bank. In this section, a number of different scenarios are used to clarify the ways in which the proposed software architecture can reduce the various types of impersonation in online assessments.

4.5.1 Fighting Type A impersonation threats

According to Apampa et al. 2010, Type A impersonation threats are associated with invigilated assessments. These threats are characterized by the involvement of the invigilator in the commission of the offence, where the invigilators collude with the student for the impersonation to happen (Weippl, 2005). This is illustrated in Figure 4.12a.

According to Gathuri et al. (2014), the invigilator / official can illegally participate in various ways including offering to assist the student with the actual assessment, allowing another person to take the assessment in place of the student, taking the assessment (provide answers by, say, pointing out correct options on the screen)., be accessible to the student and be able to view the questions and using messaging systems to exchange assessment-relevant information with the student.

This type of impersonation can easily go undetected because of the corruption of the trusted official and the ease with which passwords and information can be exchanged today (Bowness, 2016).

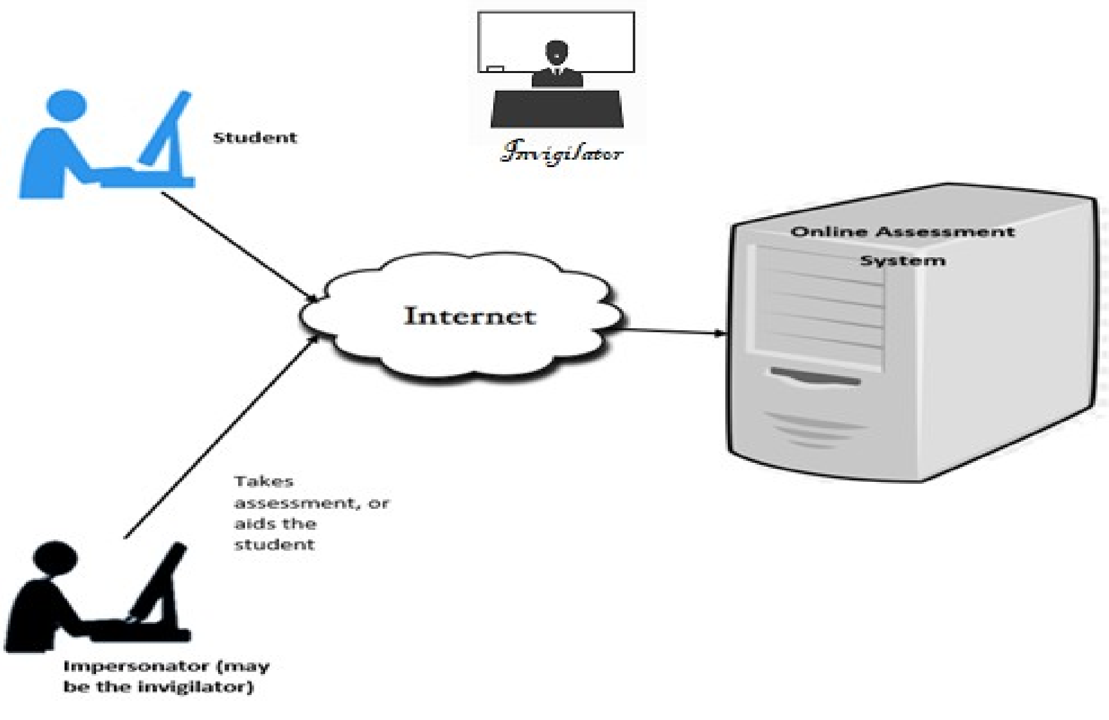

Student
Invigilator
Online Assessment System
Internet
Takes assessment, or aids the student
Impersonator (may be the invigilator)

Figure 4.12a: Type A impersonation

The proposed architecture reduces the chances of connived impersonation happening.

1. Through the *Secure Facility Unit* (SFU), the student's computer is remotely quarantined before the assessment commences. The proposed system uses behavioural biometrics from mouse and keyboard dynamics, giving the student an identity that cannot be duplicated. By blocking other unwanted applications such as instant messaging applications, prohibiting screen sharing, clipboard functions such as copy, cut, paste, screen shooting, printer and browser locking, the architecture provides a way of reducing impersonation of Type A. This prevents the student from divulging the contents of the assessment to other parties.

2. In the case that the invigilator attempts students to switch their places or substitute each other, the *One-Time Password Manager* (OTPM), SRE, and Student *Location Engine* and the MAE can detect the anomaly and flag the impersonation even if the impersonator is in a different location and remote invigilation is used (Figure 4.12b).

The time restriction on capturing the OTP and matching student recognition by the Student Recognition Engine reduce opportunities for Type A impersonation. The Multifactor Authentication Engine provides a mechanism of reading and verifying biometric variables continually through randomly timed recognition processes e.g. capturing still photos and video.

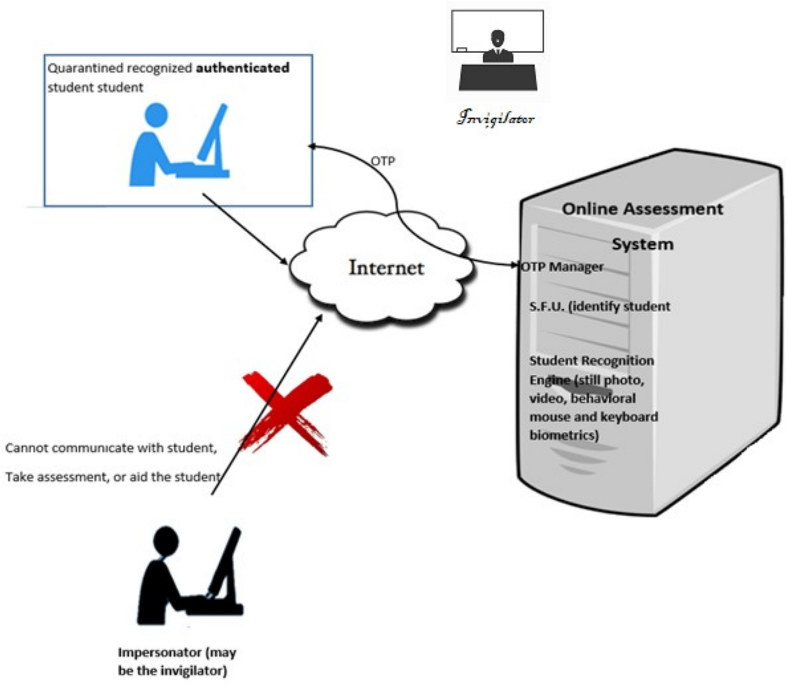

Quarantined recognized **authenticated** student student
Invigilator
OTP
Internet
Online Assessment System
OTP Manager
S.F.U. (identify student
Student Recognition Engine (still photo, video, behavioral mouse and keyboard biometrics)
Cannot communicate with student, Take assessment, or aid the student
Impersonator (may be the invigilator)

Figure 4.12b: Fighting Type A impersonation

4.5.2 Fighting Type B impersonation threats

Type B impersonation can happen when the student has divulged the credentials to an impersonator (Bowness, 2016). Figure 4.13 illustrates how this would happen in an online assessment system.

1. The impostor correctly enters the log in details (as provided by the student) and gains access to the assessment with all system indicators within the system, regarding them as the legitimate student.

2. Given that valid student identity or log in credentials are captured, focus shifts to proving that the student is who they claim to be (as per the captured credentials such as username and password).

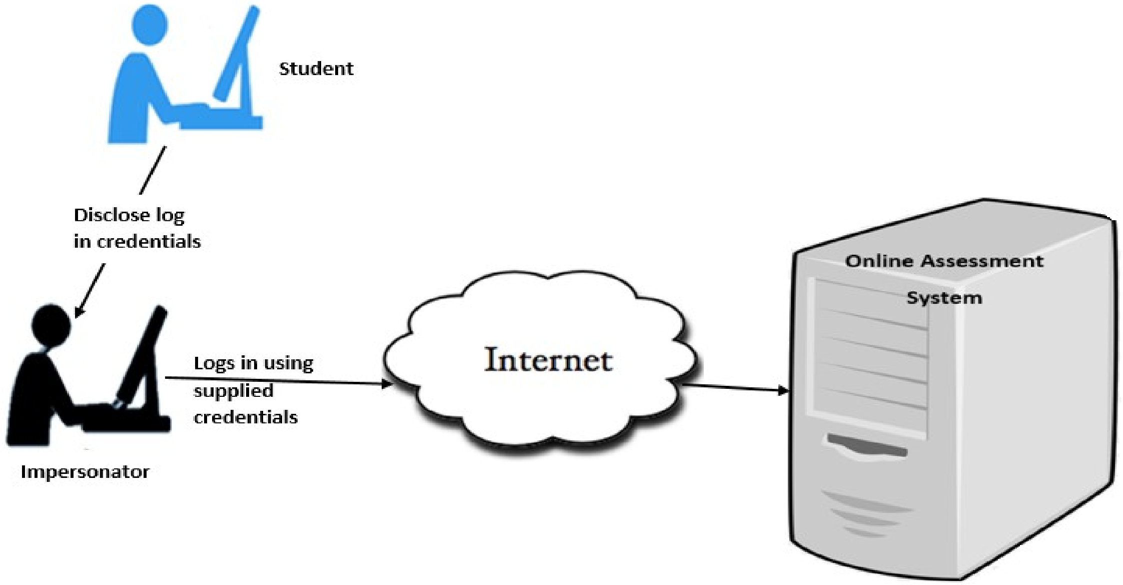

Student
Disclose log in credentials
Impersonator
Logs in using supplied credentials
Internet
Online Assessment System

Figure 4.13: Type B impersonation

The proposed architecture can fight Type B as follows:

1. From the time the assessment session begins, the Multifactor Authentication Engine (MAE) listens to the inputs captured into the user's system from hardware such as the keyboard and the mouse. B*iometric data capture devices* that include microphone, still photography and motion video also capture data for monitoring the student's actions and environment.

2. Continuous listening and processing of authentication data captured from the user, establishes the identity and presence of the user, through behavioural patterns such as typing “habits or rhythm” and mouse mobility.

3. The engine runs this process throughout the assessment and extends the mechanisms used to authenticate the student, beyond the basic username and password used at the start of the assessment session.

4. This continuous monitoring of the student’s authentication data increases the security of the assessment from impersonation and reduces the probability of another person using the assessment system, purporting to be the legitimate student. These tools and features of the proposed system will catch the would-be impersonator. This is shown in Figure 4.14.

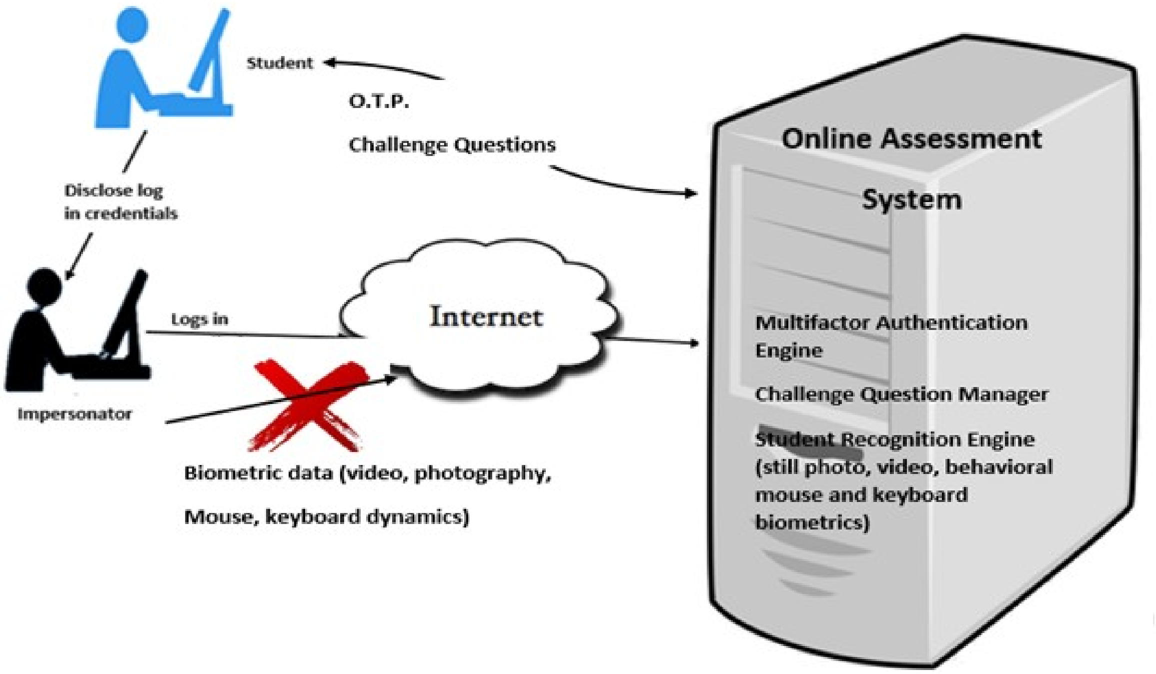

Student
O.T.P.
Challenge Questions
Disclose log in credentials
Logs in
Internet
Impersonator
Biometric data (video, photography, Mouse, keyboard dynamics)
Online Assessment System
Multifactor Authentication Engine
Challenge Question Manager
Student Recognition Engine (still photo, video, behavioral mouse and keyboard biometrics)

Figure 4.14: Fighting Type B impersonation

4.5.3 Fighting Type C impersonation threats

Type C impersonation occurs when the real student just logs into the assessment system and then facilitates another person to continue the assessment under his or her name (Apampa et al., 2010). This type of impersonation poses the most serious challenge to online assessment security. Type C impersonation (Figure 4.15) means that the valid student identity is provided and yet a different person then takes the assessment.

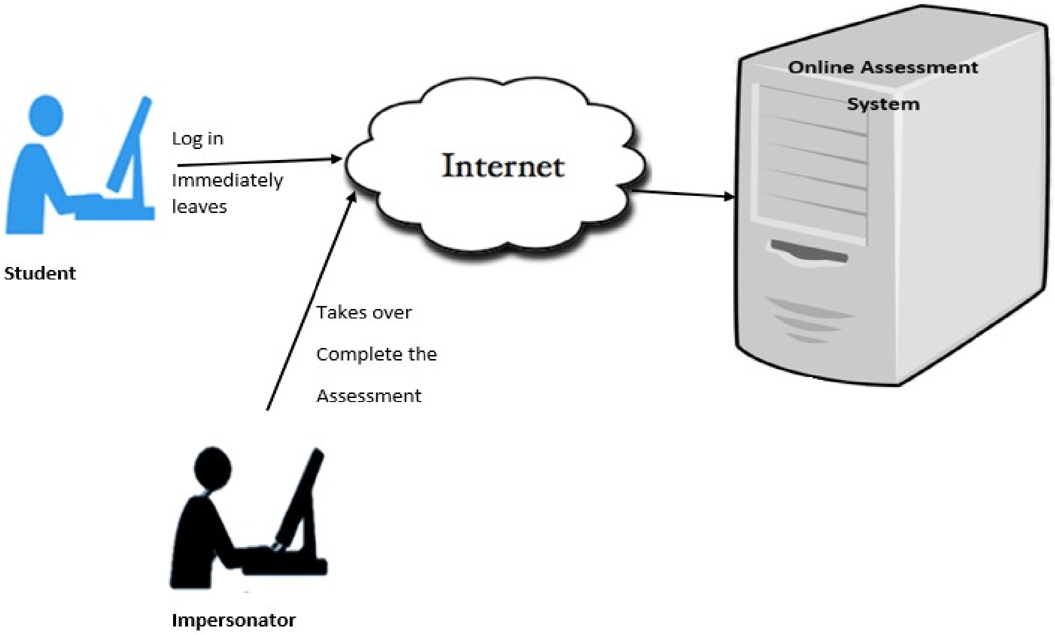


Figure 4.15: Type C impersonation

To reduce Type C impersonation, the proposed architecture uses the following approaches (Figure 4.16):

1. *Challenge Questions:* These questions could be spaced between sections in the assessment and correct answers to give the required authorization to proceed or submit the assessment (Ullah et al., 2014). If incorrect answers are given, the assessment cannot proceed to the next section and if this happens at the end of the assessment, the system would refuse to submit the assessment.

2. Continuous presence checking through biometric authentication.

    a. The proposed architecture has a secure facility unit that provides the ability to capture events like live videos, audio recordings and still photography as ways to establish that the student is taking the assessment.

    b. Facial recognition and motion picture facilitate continuous authentication of the person taking the assessment by either using remote invigilators or Artificial Intelligence Unit.

c. Tracking the behaviour of the user continuously through mouse and keyboard dynamics, provides further means by which the student can be authenticated as the legitimate candidate for the assessment.

d. The One-Time Pin Manager (OTPM) and Student Locator Engine (SLE) technologies provides a means of fighting against Type C impersonation that can potentially involve people who are not in the same geographical space by mapping the location of devices, such as the cellular phone and the venue from which the assessment is happening.

e. The implementation of these predicative OTP and SLE technologies plus immutable biometric attributes such as facial and other biometric authentication as proposed in the architecture, mean that the equipment used to start and attempt the assessment must be in the same place and continuous authentication during the assessment further complicate Type C impersonation.

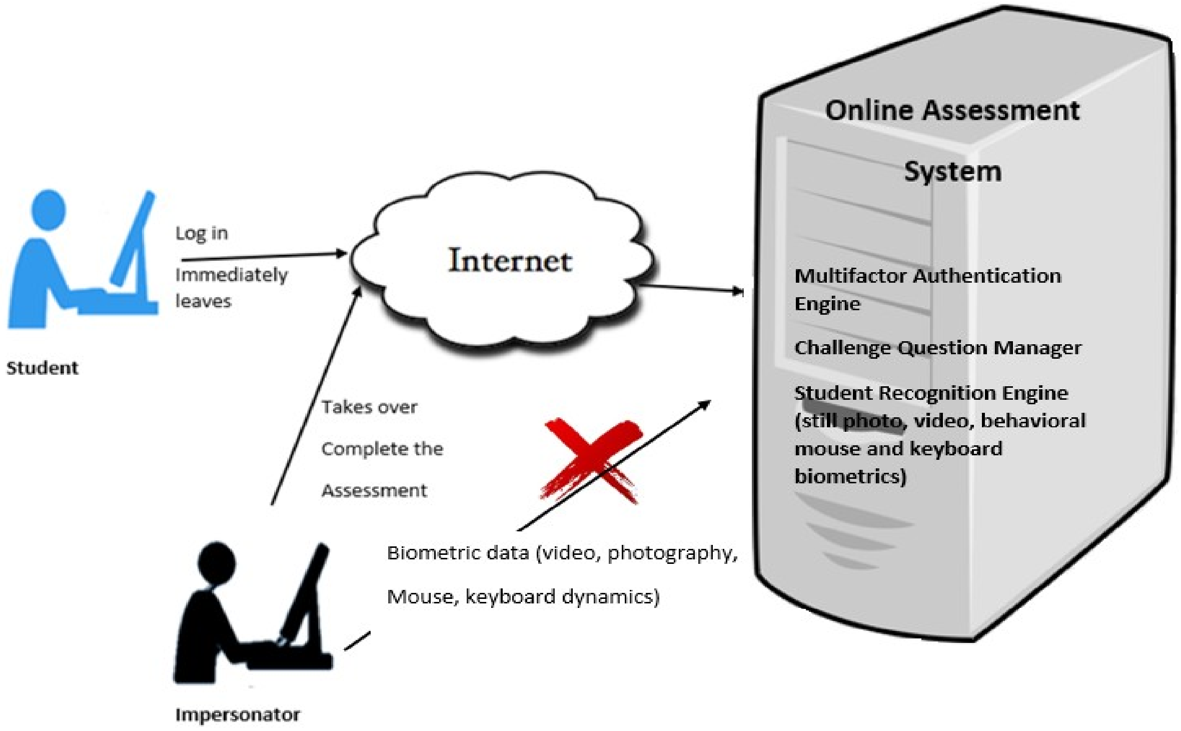

Log in
Immediately leaves
Student
Internet
Online Assessment System
Multifactor Authentication Engine
Challenge Question Manager
Student Recognition Engine (still photo, video, behavioral mouse and keyboard biometrics)
Takes over
Complete the
Assessment
Biometric data (video, photography,
Mouse, keyboard dynamics)
Impersonator

Figure 4.16: Fighting Type C impersonation

4.5.4 Fighting Type D impersonation threats

This Type D occurs when the real student logs onto the assessment system and takes the assessment. However, impersonation happens because the answers submitted are from the student working in a cohort with a third party (Apampa et al., 2010; Sabbah et al., 2011). This may happen when the student and the third party are in the same physical space or geographically apart i.e. connected in Cyberspace. Figure 4.17 shows this first way in which Type D impersonation can take place in an online assessment.

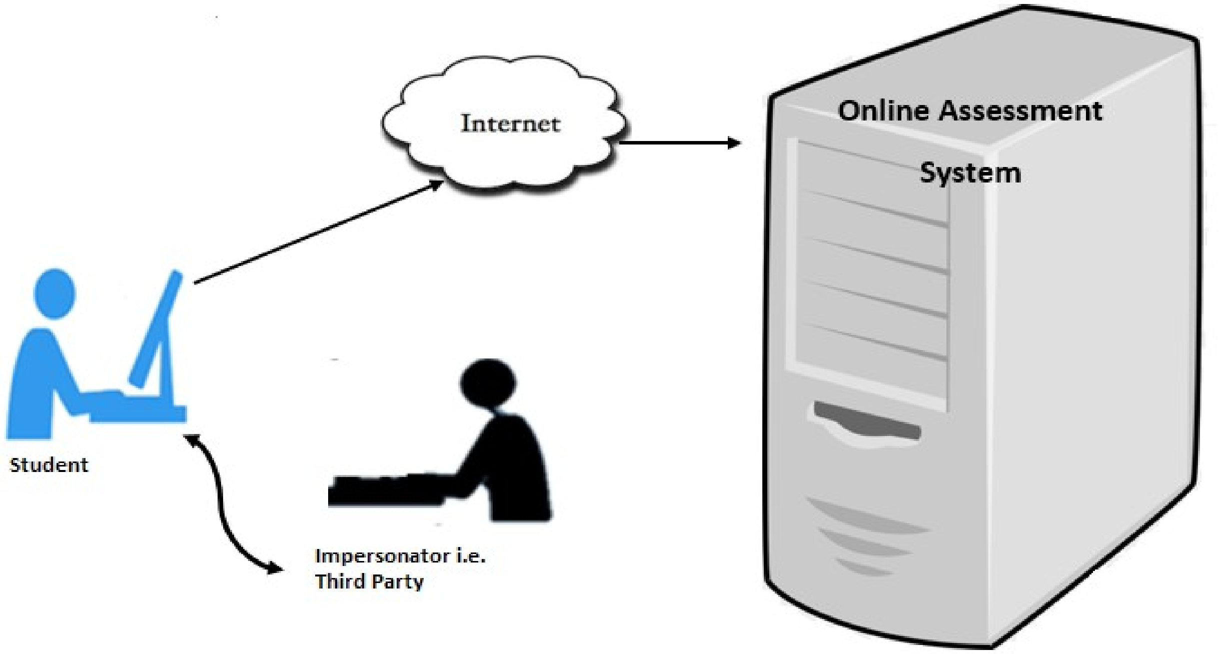


Figure 4.17: Type D impersonation in the same space

Type D impersonation can also happen when the student and an accomplice interact electronically through technologies such as screen shooting, duplicate screens, remote desktop, telephonically, instant messaging via social media, or screen and desktop sharing technologies. The second way by which Type D impersonation can happen is shown in Figure 4.18.

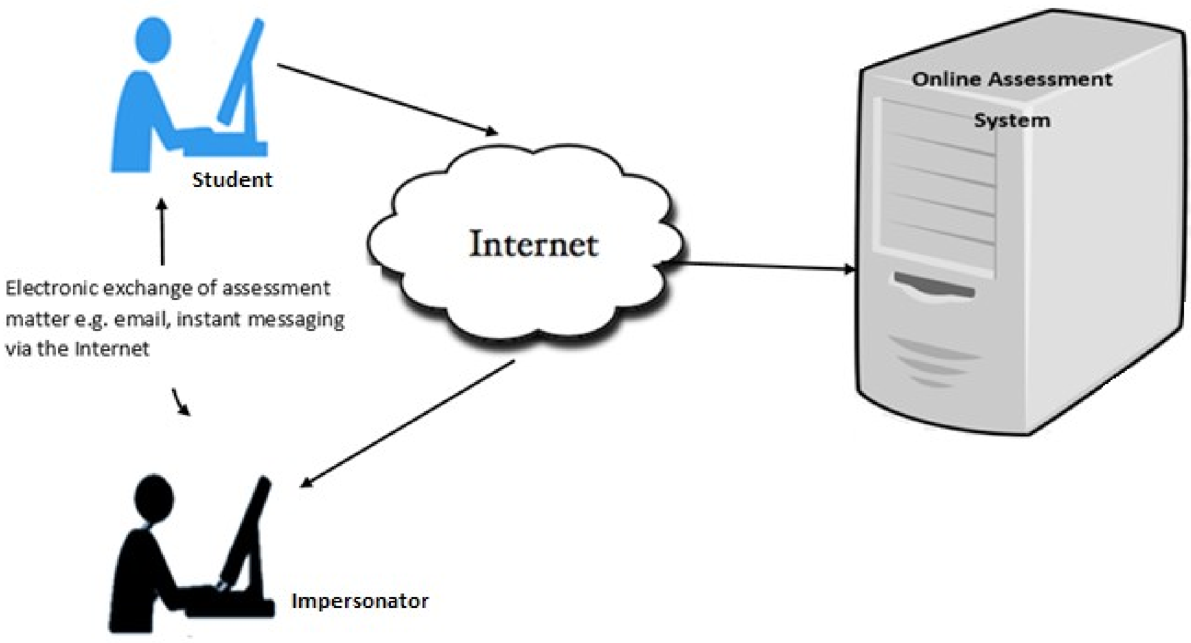

Student
Online Assessment System
Internet
Electronic exchange of assessment matter e.g. email, instant messaging via the Internet
Impersonator

Figure 4.18: Type D impersonation in cyberspace

The proposed software architecture reduces Type D impersonation as explained below.

A. Impersonation in the same space

The following processes are engaged to combat this first type of impersonation that involves the student and impostor being in the same physical location.

1. The audio and video monitoring provide an easy way of monitoring what happens in the assessment environment by capturing images, 360-degree video of the student's space, facial video from the webcam and sound. See Figure 4.19.

2. Artificial Intelligence can be included to monitor head and eye movements and determine the point of focus – this *must be the screen* for a substantial amount of assessment time. If the student's point of visual focus is deemed to be behind or past the screen, the presence of an accomplice assisting the student can be suspected (Lu et al., 2017).

3. These basic technologies enable faculty staff to monitor events on the student's site and intervene as necessary. The technologies in themselves create evidence should the student cheat.

4. Using these technologies with the student's awareness also serves as a deterrent to such practice.

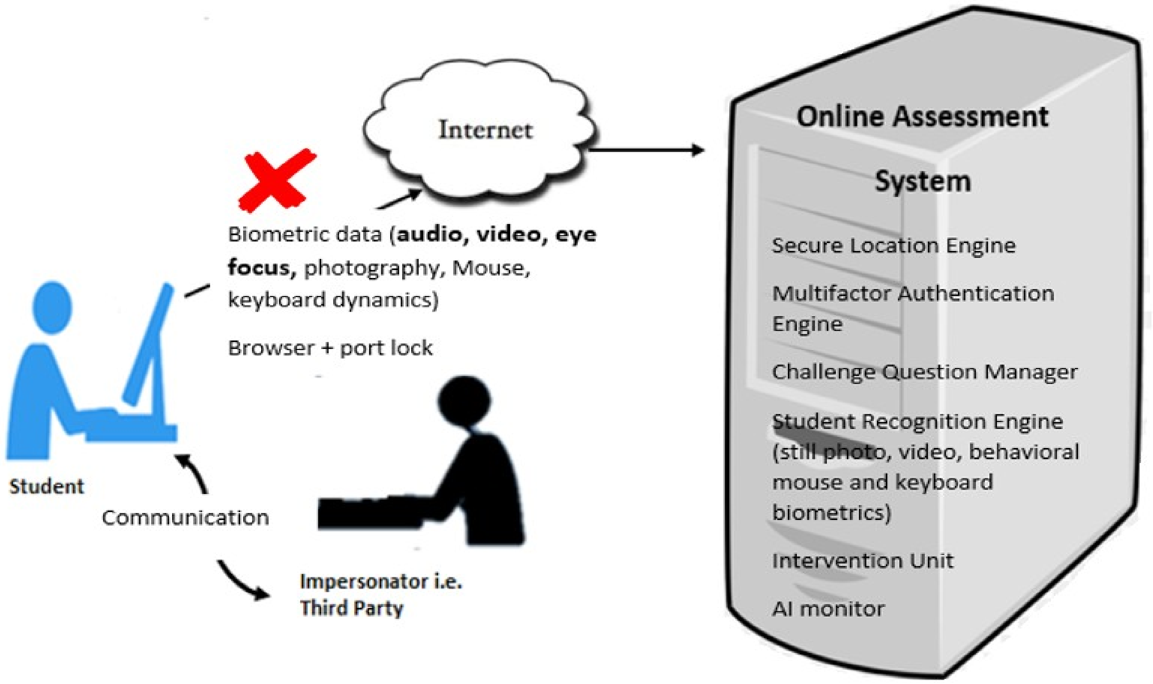

Internet
Biometric data (**audio, video, eye focus,** photography, Mouse, keyboard dynamics)
Browser + port lock
Student
Communication
Impersonator i.e. Third Party
Online Assessment System
Secure Location Engine
Multifactor Authentication Engine
Challenge Question Manager
Student Recognition Engine (still photo, video, behavioral mouse and keyboard biometrics)
Intervention Unit
AI monitor

Figure 4.19: Fighting Type D impersonation in the same space

B. *Impersonation in cyberspace*

To reduce opportunities for this type of impersonation, the assessment system follows a different process:

1. The OTP mechanism and the student location engine establish a link between the locations of the student computer used in the assessment, the student's registered personal phone. This information gives a method of verifying that they are in the same geographical location. The link is established through the Media Access Control (MAC) address and the General System of Mobile communication (GSM) and Global Positioning System (GPS) technologies.

   This connection is useful in preventing the transmission of vital data such as OTP to a distant party for purposes of impersonation. The OTP mechanism can be used at the start, between sections and as the final submit process at completion. GPS tracking can assist in trapping suspicious events that may happen.

2. During the assessment, the Student Location Engine in the proposed architecture provides continuous location verification by periodically polling the student's phone,

probing for location data. This data provides a thread or trail that can be used to monitor the location of the devices throughout the assessment.

3. The Audio-Video Manager and student recognizer provide a mechanism of checking the sound and give a view (still photograph) or 360-degree live video of the student during assessment. This deters the interaction (such as the use of a cellular phone) between the student and another party through voice and signalling.

4. Type D impersonation is further reduced by the Secure Facility Unit (SFU), which remotely controls the peripherals and software on the student’s computer. See Figure 4.20. These controls quarantine the student by:

   i. Locking the browsers on the student’s computer so that access to online exchanges become impossible and the student cannot source answers from unauthorized online sources.

   ii. Port locks block electronic access to the student’s computer. This means that technologies such as printing the assessment, screen duplication, instant messaging cannot take place between the student and other parties.

5. The intervention unit allows faculty or Artificial Intelligence to continuously monitor the student during the assessment e.g. the student’s posture, head, and even eye motions to ensure that the student is not assisted from behind the monitor in the blind spot of the web camera.

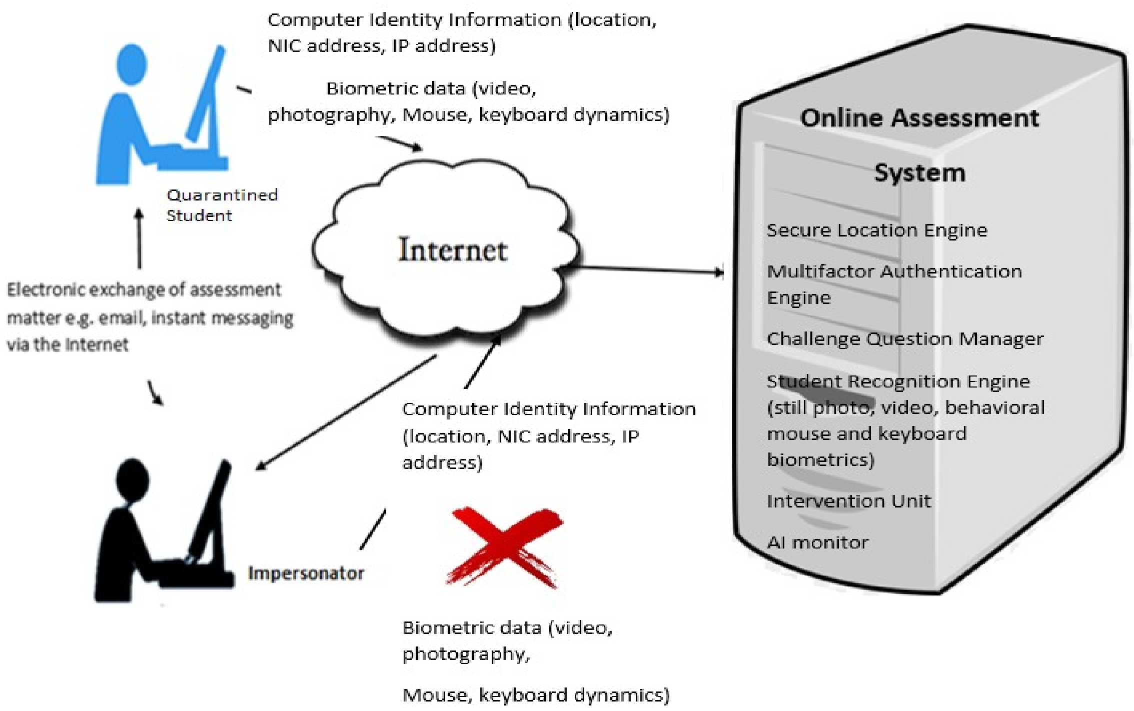

Computer Identity Information (location, NIC address, IP address)
Biometric data (video, photography, Mouse, keyboard dynamics)
Quarantined Student
Internet
Online Assessment System
Secure Location Engine
Multifactor Authentication Engine
Challenge Question Manager
Student Recognition Engine (still photo, video, behavioral mouse and keyboard biometrics)
Intervention Unit
AI monitor
Electronic exchange of assessment matter e.g. email, instant messaging via the Internet
Computer Identity Information (location, NIC address, IP address)
Impersonator
Biometric data (video, photography,
Mouse, keyboard dynamics)

Figure 4.20: Fighting Type D impersonation in cyberspace

4.6 Aggregated stakeholder concerns

After consolidating, aggregating and analysing stakeholder concerns, the central concerns raised by the stakeholders are shown below. Table 4.2 shows the 7-point Likert scale that ranks stakeholder concerns by importance.

Table 4.2: A 7-point Likert scale for stakeholder concerns

Rank / Value	Description
1	Not at all important
2	Low importance
3	Slightly important
4	Neutral
5	Moderately important
6	Very important
7	Extremely important

Table 4.3 summarizes stakeholder concerns using the scale described in Table 4.2.

Table 4.3: Pre-ATAM stakeholder concerns

Stake Holder group	**Concerns**								
	Privacy	Security	Availability	Reliable	Cost	Compatible with LMSs	Usability	Scalable / Robust	Speed/ Response
Student & parent	7	7	7	7	7	3	7	2	7
Faculty	6	7	7	7	5	6	5	4	5
Quality management	6	7	7	7	5	6	6	5	5
Information systems	6	7	7	7	6	7	5	7	7
Policy making	6	7	7	7	7	5	5	3	7
Total Score	**31**	**35**	**35**	**35**	**30**	**27**	**28**	**21**	**31**

The stakeholder concerns that are shown in Table 4.3 and architectural design decisions are used to create a proposed software architecture for an online assessment system that reduces impersonation in online assessments.

4.7 Evaluation of software architecture

Software architecture design is a stakeholder-centred activity; it is therefore important that stakeholders endorse the design before the software is physically developed. The software architecture design is submitted for evaluation by the various stakeholders – each stakeholder validating or disputing the design in the context of their own concerns. The Architecture Trade-off Analysis Method (ATAM) was used to evaluate the design with the stakeholders. According to Montenegro et al., (2017), the ATAM is comprised of the process steps shown in Figure 4.21.

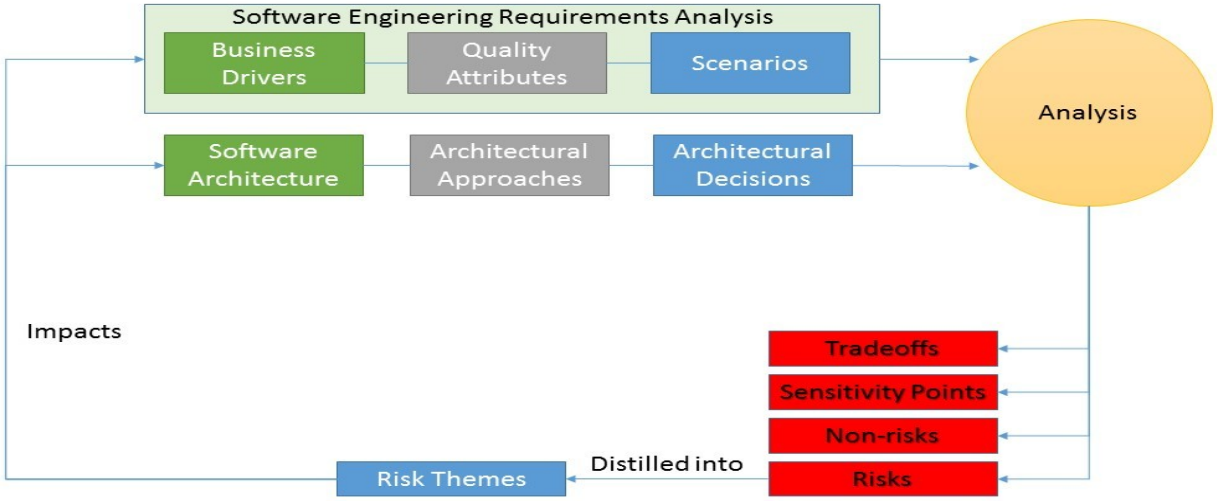


Figure 4.21: Architecture evaluation using ATAM

The stakeholders were engaged in the evaluation of the proposed architecture using the Architectural Trade-off Analysis Method (ATAM), described in Section 3.12.

The ATAM process revolves around iteratively analysing each stakeholder's use scenario and identifying trade-offs among stakeholder concerns, sensitivity points, the risks, (and non-risks). In each iteration, the principles and approaches of software architecture lead to certain architectural decisions (Montenegro et al., 2017).

The risk themes from the previous iteration and the architectural decisions interact in each cycle, and possible designs yielded in subsequent cycles. Montenegro et al. (2017) explain that the ATAM cycles continue until an architectural definition that is acceptable to the stakeholders is achieved, or other project control parameters such as time or budget run out. This would cause other decisions to be made by the sponsor or management.

The ATAM is a technique that can be used to collect data about stakeholder concerns, in light of a proposed architectural definition, applying the performance scale discussed in Section 4.2, the proposed architecture scores as shown in Figure 4.22.

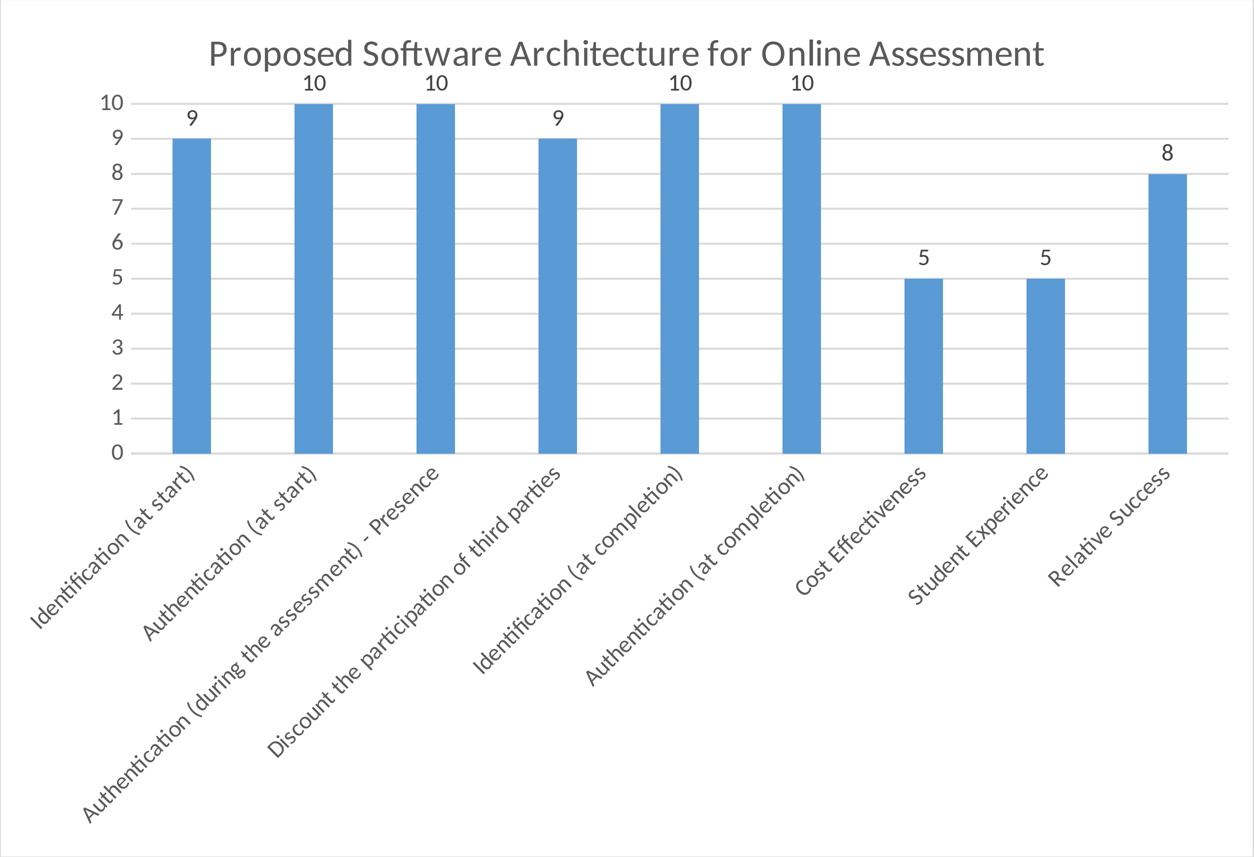


Figure 4.22: Projected performance of proposed architecture

4.8 Chapter Summary

By closely following the methodology laid down in Chapter Three, stakeholders were identified and the concerns of each stakeholder group were condensed to define a software architecture. The functional and non-functional requirements of the stakeholders were clarified using scenarios and criteria for measuring the performance of online assessments.

Stakeholders agreed that online assessment systems could be evaluated and rated in terms of some metrics that point to the system's ability or potential to reduce impersonation. These metrics are reflective of the effectiveness of each system's ability to provide security against impersonation. These metrics measure the system's performance in the identification and authentication of the student at various times. Identification and authentication take place when the assessment begins, continually during the assessment and at the conclusion of the assessment as part of the submission process. Such continuous authentication provides a method to keep track of the presence and participation of the student throughout the assessment and can reduce opportunities for the participation of third parties.

Factors such as the initial identification, continuous authentication, cost effectiveness, student experience, and estimated likelihood of success against impersonation were used as parameters the “design a software architecture” stage for an online assessment system and to compare the design against other systems.

Based on these metrics, the ideal online assessment system would be expected to fully prevent impersonation from occurring in online assessments by perfectly delivering on all the listed metrics i.e. deliver 100% percent defence against impersonation.

The venue-based, physically invigilated online assessment that examines students in cohort at a central facility can be estimated to reduce impersonation by 90%, owing to the presence of a human invigilator who inspects identification at the start and maintains conducive assessment conditions throughout the assessment process. This option’s ability to fight impersonation is weakened by the possibility of collusion between students during assessment and the potential involvement of the assessment officials in influencing the outcome.

Non-invigilated online assessment systems permit the student to take the assessment at any location and at any time without any policing. These conditions make the assessment open to impersonation as they have a high reliance on the honesty and ethics of the student. The study associated this type of assessment at 50% estimated success against impersonation.

Remotely invigilated online assessment systems make use of a special suite of software such as ProctorU and Kryterion, and a designated invigilator who monitors student activity during the assessment via video and audio feeds. The study conformed the conclusion of published literature that these methods commonly include some level of interaction with a remote human invigilator in a question and answer session and the invigilator may have access and powers to control the student’s computer. The method of remote human invigilation is expensive since the invigilation service is billed separately and requires high grade hardware and software. The intensive involvement of a human invigilator takes away the student’s comfort and threatens privacy.

The proposed solution for an online assessment system that discounts impersonation permits students to take assessments from any location and at any time under software monitored conditions. The system characteristically limits human involvement in policing the assessment by making human intervention the exception rather than the norm in the running of online assessments. This reduced human involvement increases the level of privacy and confidentiality of the system compared to other human policed assessments, such as those that are venue-based or invigilated online. The proposed software system runs on institution or cloud servers, implying that the student does not require high end computer hardware and means that any internet-capable computer that has basic audio-video capability can be used. The higher dependence on software rather than human policing provides higher levels of confidentiality. On the basis of the above-named evaluation metrics, the proposed solution can potentially reduce impersonation by an estimated 90%.

CHAPTER FIVE
EVALUATION AND DISCUSSION

5.1 Overview

This Chapter builds on Chapter Four and presents the information gathered when the software architecture proposed in chapter four was presented to the stakeholders for evaluation against their use-scenarios. The process of evaluation aimed to gain clarity on the functional and non-functional requirements and shed light on the architecture proposed in terms of the trade-offs, risks and sensitivity points in relation to the online assessment system.

5.2 Evaluation of the software architecture

The design tools and documents presented in Appendix C to define the proposed software architecture formed the basis on which the stakeholders participated in the evaluation of the proposal. The definition drew stakeholder's attention and provided a vehicle for further clarification and prioritization of concerns. Their comments and more concerns captured the possible strengths and weaknesses of the architectural design. This Chapter presents a summary of the findings emanating from the stakeholders' participation in ATAM.

5.3 Architectural Trade off Analysis Method Feedback

5.3.1 The positives of the proposed architecture

The proposed architecture for secure online assessment presents an estimated 95% effectiveness against impersonation. This is a result of the following strengths and capabilities:

5.3.1.1 Integrity / Fairness of assessment

The proposed architecture combines many techniques and technologies such as encryption, multifactor authentication to safeguard the integrity of the assessment. The use of a large layered question bank makes it plausible that students taking assessments for the same qualification take a balanced and fair assessment such that the outcomes can rank their capabilities fairly.

5.3.1.2 A complete visibility of the student in assessment

The proposed architecture provides a view of the student in assessment from the webcam and from a strategically positioned phone or video camera. This provides a view of the student as they work the assessment and also a means of monitoring their environment for possibilities of third-party participation.

5.3.1.3 Any time and any place assessment

The proposed architecture aims to provide students with the added flexibility of taking assessments at a time and from any place that is convenient to them. This means that education and assessment would be free from the limitations imposed by geographical location of the student or institution and academic transactions can take place at any time.

5.3.1.4 Continuous identification and authentication

The proposed system has mechanisms for passive, continuous identification and authentication of the student from the start of the assessment to the finish of the assessment. Continuous identification and authentication of the student throughout the assessment reduces the opportunities of impersonation.

5.3.1.5 Privacy and security

The proposed system does not require the student to disclose personal information to a stranger as is the case with online invigilated assessments. For the most part, in the proposed architecture, interaction involves the student and the computer.

5.3.1.6 Quick start

The system has a basic login process that uses the student’s username and password. This means that the student can quickly engage in the assessment with little time wasted and little data transmitted to the assessment system. A simple and quick login uses less data and reduces communication costs such as broadband data charges.

5.3.1.7 Student quarantine and assessment security

The proposed architecture remotely locks down the student's computer. The hardware and software lockdown of the computer provides for student quarantine and seclusion and reduces the chances of communication and participation of third parties.

5.3.1.8 Authentication at the end of the session

This provides assurance that the students are aware that the assessment is over, and they consciously indicate that their answers are ready for evaluation and avoid premature submission. The authentication at completion is the student's sign off signal and ends the system's tracking of the student's devices and environment.

5.3.1.9 Randomized questions

The proposed architecture uses a randomized questions bank so that each student received a potentially different set of questions in each assessment. This design can guard the assessments from cohort or group cheating. Having question banks allows the institution to host assessments whenever the student wants to take the assessment i.e. the institution does not require time to develop new assessments each time students indicate readiness to take the assessment. New questions can be added to the question bank without disrupting the flow of activity in the assessment system.

5.3.1.10 Multifactor authentication

The architecture draws on the benefit of multifactor authentication which leads to a high likelihood of correctly identifying the student compared to the use of single authentication methods. Having more than one authentication mechanism in place increases the security and reliability of the system.

5.3.1.11 Faculty involvement

The architecture accommodates faculty involvement in the assessment through the webcam and microphone on the student's computer, and the second video live feed channel from the student's camera phone. This provides the ability for live human invigilation. The same video and audio feeds into the Artificial Intelligence unit to further secure the assessment against impersonation.

5.3.1.12 No software installation

The proposed architecture does not require the student to install, nor does it install any new software on the student’s computer. This means that any device that can access the Internet and provide mouse and keyboard support can be used for the assessment. This feature makes it easy, with faculty consent, for the student to change equipment in the event of hardware failure. When the switch happens, the old session ends and the new one starts at the same point, with questions reshuffled, but answers entered thus far on record.

5.3.1.13 Breaks

The provision for start / stop of assessments e.g. when the student takes a break for natural reasons or experiences a communication or power outage, makes this a sound solution for lengthy assessments such as board certification assessments that can run for hours. The architecture has the capacity to start a new session for the student, resuming from the last interaction with the correct assessment timer settings.

5.3.2 The negatives of the proposed architecture and stakeholder concerns

5.3.2.1 Privacy

The proposed architecture provides for the institution having access to the student’s computer. This raised privacy concerns as this exposes all their data to possible access and exposure. The use of two live video feeds and an audio feed across the Internet may be considered excessive and an invasion of privacy, given that the institution also holds biometric student data on its servers.

5.3.2.2 Inadequate prevention of impersonation

Despite providing a means for remote invigilation, stakeholders felt that the proposed software architecture is inadequate in the face of impersonation, especially where the students take assessment from dispersed locations. Some stakeholders pointed out the possibility of students using mirrors to image the screen for the impostors to view and wearing tiny earbuds to listen into the answers from the other parties. They argued that other cues could still be used to obtain assistance from a knowledgeable third party positioned outside the camera view zone or “blind spot” and not interacting with the student’s hardware. Google glasses™ were specifically referred to as a tool that students can use to access information from external sources. This demands vigilance on the part of faculty in carefully studying what students wear when they appear for the assessments.

5.3.2.3 Other channels: sharing assessment answers

Stakeholders proposed that, together with the browser, the student’s mobile phone must be locked upon login to avoid the exchange of messages with external persons and also enable the student to focus on the assessment. The proposed architecture requires that the student’s mobile phone be kept on and capturing a second channel feed for monitoring the student’s environment.

5.3.2.4 Question bank security, size and randomized questions

The main concern emphasized by the quality stakeholders was that the system must provide fail proof defences against hacking. Encryption, large question banks and robust randomizing algorithms are necessary for the success of the proposed system.

5.3.2.5 Challenge questions

The need to ensure that the student registered for the course and took the assessment featured prominently across stakeholder groups to emphasize, a suggestion to use challenge questions from the student’s profile at the time of registering for the assessment (Ullah et al., 2014). A different set of security challenge questions during the assessment got stakeholder attention as a good deterrent to possible substitution of the student by an impersonator.

However, parents and students did not support the use of challenge questions during the assessment as they argued that challenge questions that had no contribution towards the outcome of the assessment disrupted the focus of the students e.g. when placed within the assessment time window.

5.3.2.6 Cost

The proposed software architecture requires the student to have computer equipment and a cell phone that has a good camera and to provide a second channel feed to the assessment system. This cost may be excessive on the student.

5.3.2.7 Third party involvement

Technical stakeholders argued that the proposed architecture does not completely eliminate the participation of third parties, for instance, the party that hosts videoconference services. The security of the system is affected by the security of the quality of service and security of the third party.

5.3.2.8 Course or program level impersonation

The proposed architecture cannot detect or prevent impersonation that takes place at course level and the impostor registers and takes the course for another person under their name.

5.3.2.9 Usability

The proposed online assessment system fights impersonation using various biometrics including keyboard and mouse mobility. An argument presented by some stakeholders is that this system would be more effective in assessments that make extensive use of these devices and leave it minimally useful in assessments that involve little typing but largely involve choosing options, or cases where other devices such as touchscreens, pens and wands are used to capture input.

5.4 Post Architectural Trade off Analysis Method - Aggregated concerns

The ATAM was used together with Software Engineering Requirements Analysis to collect data from the stakeholders. The collected data was consolidated, aggregated and analysed to crystallize the concerns of the stakeholders. The following subsections summarize the central concerns raised by the stakeholders.

5.4.1 Trade-offs

A trade-off point is a property that affects two or more quality attributes and is a sensitivity point for two or more attributes. Stakeholders engaged in ATAM sessions negotiated with each other; clarifying and compromising their values and concerns.

5.4.1.1 Privacy versus security

The system's security interests of the quality and policy groups have to fit in with the personal privacy and security concerns of the parent and children groups. Policy makers require a high level of security and accuracy in delivering credible assessments to genuine students and parents and students value the privacy and confidentiality of their private space and interactions.

5.4.1.2 Faculty involvement versus faculty intervention

One of the major types of impersonation, also one that is difficult to detect is impersonation that involves an assessment official or invigilators. A crucial requirement of Faculty is an ability to monitor assessments and having the capacity to intervene should the need arise.

This requirement presents a potential conflict between the software-intensive system's constraint to reduce human involvement and the stakeholder requirements. Prudent and responsible behaviour plus other policing systems are necessary to make the solution usable in online assessments.

5.4.1.3 Conclusiveness of evidence versus transmission costs

The proposed architecture envelopes all data transmitted from the student's computer with information that distinguishes the student, the cellular phone, computer and the location of the device(s). This constitutes a bundle of data which can raise the costs of transmissions. On the other hand, the design targeted to provide a comfortable and affordable assessment experience.

5.4.2 Risks

The architectural risks, sensitivity points, and trade-off points of the architecture were exposed and explored to determine the suitability of the chosen architectural approach. The risks, security points and trade-offs of the proposed solution are subject to the preferences of the participants and cannot be considered universal and applicable to all possible situations and settings.

5.4.2.1 Good student behaviour

The design places the onus of choosing a good time and place for assessment on the student. This poses the risk of reducing the institution's control of the variables of time and place that assessments may happen.

Interventions and monitoring efforts supported by humans become less effective as physical and time differences increase. For example, on the final day of the assessment window when all outstanding students attempt the assessment in potentially huge numbers and faculty may be overwhelmed.

5.4.2.2 Privacy and security of student data

The architecture requires the collection and retention of biometric data about students. This poses the risk of exposure through hacking and carelessness of those in custody of the data and so forth. This risk demands that institutions install stringent measures to protect the data from unauthorized access. Averting this risk of loss or disclosure of data is associated with an increase in setup and running costs of a system. Data Laws provide some safeguard against this risk, thus institutions need to be aware of these Laws and conduct all activities in accordance with the stipulations of the Law.

5.4.2.3 Hardware performance

The design requires functional audio-visual equipment in the student's computer to capture sounds, pictures and video for authentication and monitoring purposes. This presents a risk when the equipment fails on its own. Further, impersonators may tamper with the equipment and create the impression that the equipment is failing. This poses a risk, in that the system does not have a method of determining genuine faults and places the institution in a position where they need to design and engage other methods to facilitate investigation and possible re-assessment.

5.4.2.4 Internet and hardware performance

The continuous authentication described in the design requires optimally performing hardware and a good quality internet connection i.e. a connection that is uninterrupted, fast and secure. A break or deterioration in the connection quality can cause serious problems with the assessment.

5.4.3 Sensitivity points

A sensitivity point is a property of one or more components and their interrelationships that is essential for the achievement of a specific quality attribute or response. This results from having many classes of stakeholders with each class having a different priority for the concerns can cause conflicts and potential implementation challenges.

5.4.3.1 Hardware readiness and quality of performance

The architecture design requires the hardware that will be used for assessments to be ready and functional at the commencement of the assessments. Equipment such as cellular phones and mobile computers that require power must be made ready ahead of assessment time. The mechanics described in the architecture require the availability of all the hardware at various points in time. It is vital that each component be ready when it is required to ensure the availability of the authentication services and security of the assessment.

The hardware must provide a level of service that provides enough evidence to conclude on the quality of the assessment or proof of academic fraud should any occur. For instance, the audio and visual equipment on the student's computer must deliver good quality sound, picture and video.

5.4.3.2 Connectivity

Students can access assessments via Wi-Fi or Ethernet connections. There is a need for the internet connection to be functional throughout the assessment and the cellular phone used for verification must also be functional and "reachable" on its network. Failure in any of these cases can harm the assessment or the student's assessment experience.

Assessment data can be considered "highly sensitive" and as such, the connection used must be secure. Table 4.2 explained the seven-point Likert scale that ranks stakeholder concerns by importance. Table 5.1 summarizes stakeholder concerns using the scale described in Table 4.2.

Table 5.1: Post- ATAM stakeholder concerns

Stake holder	Concerns								
	Privacy	Security	Availability	Reliable	Cost	Compatible with LMSs	Usability	Scalable / Robust	Speed/ Response
Student & parent	7	7	7	7	4	4	4	2	7
Faculty	3	5	7	7	4	5	3	6	5
Quality Mgt	3	5	7	7	4	5	3	6	5
Info. Systems	3	6	7	7	3	3	3	6	6
Policy making	2	4	7	7	3	4	3	4	6
Total Score	**18**	**27**	**35**	**35**	**18**	**21**	**16**	**24**	**29**

The stakeholder concerns, architectural design principles and architectural decisions were used to create a proposed software architecture for an online assessment system that reduces impersonation in online assessments without imposing extra costs on the student or the institution.

The post-ATAM ratings presented in Table 5.1 relate the extent to which the items listed in the header row concerned the stakeholder. A comparison of Table 4.3 and Table 5.1 shows significant reductions in the Total Score row for some different concerns such as security and cost across the stakeholder community. The reductions indicate measurement of the extent to which the stakeholders saw the potential of the proposed architecture to deliver an online assessment system that could reduce impersonation in online assessments. The reduction in the cost of having a secure online assessment system is one of the primary targets of the research project.

5.5 Chapter Summary

Software architecture is a feasible method for the design of a software solution that can discount or reduce impersonation in online assessments taken at Higher Education level. Of vital importance is the need to have adequate security when the student logs onto the assessment and high security should persist throughout the assessment. These requirements must be met at a cost that is within the reach of the student and also the institution. Multifactor authentication provides methods by which impersonation can be reduced. Large question banks, robust randomizing algorithms and remote invigilation can be implemented using technologies such as video and audio monitoring, behavioural biometrics and Artificial Intelligence. Facilities for faculty intervention should students breach security, further deter students from attempting impersonation as a means to academic fraud.

CHAPTER SIX
CONCLUSION AND FUTURE WORK

6.1 Summary

The primary objective of this research was to design a software architecture for an online assessment system that reduces impersonation. A systematic literature review guided by the works of Kitchenham et al. (2010) revealed the ways by which impersonation happens in online assessments and the major ways used to counter impersonation by verifying student identification.

Impersonation happens when a student is replaced by an impostor who possesses the information or object(s) necessary to log on to the assessment. Impersonation happens with the consent and participation of the student who allows another person to replace them in the assessment under their identity.

Strong authentication is necessary in order to secure online assessments. Many authentication technologies have been proposed to fight impersonation. Some of these technologies authenticate the student at the beginning of the assessment and others provide continuous authentication throughout the assessment. The most secure online assessment must provide continuous authentication and cause minimum disturbance to the student during the assessment. Some authentication methods require expensive hardware beyond the basic computer configuration. This makes such methods expensive and beyond the economic reach of students and institutions. Other technologies tend to be too intrusive or disruptive and therefore harm the “student assessment experience”.

This research project proposes a software intensive solution that can minimize impersonation using standard computer hardware. Providing continuous authentication and restricting disturbances on the student as the assessment takes place were the primary objectives in the design of the proposed software architecture.

In all stages, the proposed software architecture development process took the concerns of various stakeholders into account. Stakeholder concerns were collected and analysed using the principles of software engineering. These concerns and the principles of software architecture development were used to create and refine the architectural design.

A preliminary solution design to the problem of impersonation in online assessments was tabled before the stakeholders in iterative Architectural Trade-off Analysis Method (ATAM) sessions. In each iteration, the design was clarified, and stakeholders brainstormed the risks and trade-offs that existed in the sets of requirements or concerns. In the ATAM sessions, concerns were reprioritized, risks and trade-offs identified as stakeholders were engaged in evaluating the solution designs.

6.2 What this research achieved

This research defined a software architecture for an online assessment system that can reduce impersonation. The architecture defined in this work identifies a secure online assessment system comprising two major components, an Identity Management System (IMS) and the generic Learning Management System (LMS).

The identity management system is responsible for identifying and authenticating students at the beginning and throughout the assessment. Through the IMS, all interactions with the LMS are authorized.

The authentication functions of the IMS interact continually with the LMS. This enables the IMS to listen to events happening in the LMS and provide continuous authentication and authorization.

The proposed architecture defines the IMS in detail as a system that seamlessly integrates with existing LMS through an interface. This architectural design enables the learning management system and its users to operate with minimum disruption, by running much of the environment monitoring and authentication processes in the background.

The provision of a secure environment for online assessment is achieved in the following basic stages and processes:

The student initiates the assessment session by logging onto the system using a username and password pair complimented by a One-Time Password (OTP) that is transmitted through the student’s registered cellular phone.

The IMS remotely sets up the assessment environment by activating the audio and video peripherals on the student's computer. These peripherals collect identification information about the student such as voice, still pictures and video.
The IMS quarantines the student's environment by locking the web browsers, communication ports and disables clipboard for copy, cut and paste functionality on the student's computer. This measure ensures that the student cannot use the computer to browse for answers from online sources or exchange assessment matter electronically with other persons.

The architecture defines measures that monitor the assessment environment up to the completion of the assessment by monitoring processes at the student's venue (audio and video).

The architecture provides continuous student authentication using Artificial Intelligence such as facial recognition and machine learning i.e. anatomic biometric data in the form of photography and video for facial recognition, and behavioural biometric data from keyboard and mouse dynamics (Almalki, Chatterjee & Roy, 2019)

An Intervention Unit through which Faculty or Artificial Intelligence can "intervene" in the event that something out of the ordinary happens and more attention is required, provides enhanced security.

The exchange of authentication data between the IMS and LMS is a continuous process that happens throughout the assessment and is transmitted across the internet in an encrypted format.

On completion of the assessment, the student is authenticated using token-based authentication and predicative data. Final submission of the assessment involves an exchange of a text message that is sent to the student's cellular phone.

As summarized here, the architecture solution can authenticate students at the beginning, during and at the completion of the assessment and hence reduce the chances of impersonation taking place during the online assessment.

6.3 Limitations & future work

6.3.1 Privacy concerns

The primary challenge faced by the proposed architecture is the need to access and match the hardware used by the student. This is useful in ensuring that all exchanges involve the legitimate student but opens up the student's system and privacy to violation, disclosure and abuse.

6.3.2 Compliance issues

It is also necessary to note that the implementation of the architecture demands compliance with the Application Programming Interface (API) of the Learning Management Systems (LMS) that institutions use to facilitate the exchange of data in real-time between the Identity Management System(IMS) and the LMS.

The data packets that the LMS handles when augmented with IMS data may be large and can cause cost challenges for the assessment system.

6.3.3 Equipment substitution

The architecture requires that the student be equipped with computer hardware that provides audio and visual communication capability. The failure or absence of these pieces of hardware on a student's equipment seriously cripples the design.

6.3.4 Other technologies

The architecture relies heavily on the video streams augmented by keyboard and mouse "culture" of the student to identify the person taking the assessment. Exclusion of these hardware options may impose serious limitations on the continuous authentication of the student. Using early version cell phones or a touchscreen for selections and onscreen keyboards for example are not adequately addressed by the architecture.

Virtual Private Network (VPN) technology may throw off the readings obtained from the predicative data that maps to the student's computer and cellular phone locations. Demanding that students stop security measures that they may have grown accustomed to may not be favourable as it may disrupt their comforts and security outside the assessment.

6.3.5 100% course impersonation

If an impersonator registers for a course under a different name, takes the course and the assessments, the system cannot trap the academic offence because the data such as biometric data, challenge questions held on file by the institution will relate to the impostor. This means that an individual receives a qualification without ever taking the studies. The proposed software architecture is not fool proof and heavily relies on vigilant registration processes to demand proof of identity in the first place.

6.3.6 Other security risks

The proposed architecture only pays attention to and attempts to identify the hardware that a student might use when the student engages the system for assessment. This poses new challenges in the context of the security of devices on which students connect to the assessment system and enter their answers to assessment questions.

6.3.7 Limited identity management

The proposed architecture does not address concerns around how identity management would be achieved and imparted on systems where data collections are federated, where heterogeneous devices are used, or when a server-less functions and services are adopted.

6.3.8 Scalability

The information systems group queried the capacity of faculty intervention in online assessments when the volume of students taking assessments grows exponentially as is the case with Massive Open Online Courses or “MooCs”. The general opinion presented by the information systems group was that the routine security measures should be completely automated i.e. they believe that the architecture solution would be more effective without human involvement. The information systems group opined that should humans be involved, the involvement should be restricted and be under the control of the Artificial Intelligence.

6.4 Future work

Impersonation is a serious problem in online assessments. To enhance the security of online assessments and reduce impersonation at low costs to students and institutions, further study into ways in which non-intrusive, secure and continuous authentication is vital. Future study in Artificial Intelligence (AI) especially Machine Learning, Artificial Neural Networks, the Internet of

Things (IoT) to find ways of authenticating each student and their interaction with the LMS. Big Data Analytics could also be explored to create predictive technologies that can raise flags when students engage in impersonation activities during online assessment

6.5 Conclusion

This research set out to find how an online assessment system can be architecturally defined so that it reduces impersonation. Using the Design and Creation strategy (Oates, 2006), a pragmatic, stakeholder – driven and technology-independent software architecture was defined. The proposed software architecture provides for student authentication by combining knowledge-based authentication, using usernames and passwords, One-Time Pins (OTPs), predicative location finding technologies for cellular phone location, Internet Protocol (IP) addresses and the Media Access Control address (MAC) of the student computer.

The proposed architecture permits inclusion of various biometric authenticators such as mouse dynamics, video and audio streaming for both, automated and human remote invigilation. In the transmission of authentication factors, the architecture proposes encrypted data traffic, each packet emanating from the student's computer carrying answers, video, image and so forth, bearing a unique signature of the student and the hardware that it transmits (student identification information, MAC address of the computer used, IP addresses and time and location stamp).

These pieces of data are collected, packaged and transmitted in the background during the assessment session to provide non-intrusive continuous authentication of the student throughout the assessment. The architecture blocks out electronic communication with third parties, and only offers facilities for faculty and the institution to intervene should the assessment be disrupted for example, suspicious behaviour that deserves the attention of remote (human or artificial) invigilators.

The contribution made by this research is a description of a software architecture design that deliberately targets to reduce impersonation in online assessments. More research is required to further the fight against impersonation in Higher Education. In this regard, this project can conclude with the expression of hope that an online assessment that regards this architecture in its design and construction can reduce impersonation and deliver credible, dependable and secure assessments in environments that are geographically dispersed, permitting students to take the assessments at the most convenient times.

REFERENCES

Abdelhameed, R., Khatun, S., Ali, B., Ramli, A. 2005. Authentication model based bluetooth-enabled mobile phone. *Journal of Computer Science* 1(2), pp. 200 – 203.

Abnave, A., Banait, C., Chopade, M., Godalkar, S., Pawar, S. and Nikam, V., 2017. *Secure Examination Management System for M-Learning (SEMS)*, pp. 31 – 35.

Acien, A., Morales, A., Fierrez, J., Vera-Rodriguez, R. and Bartolome, I., 2020. *Be-CAPTCHA: Detecting Human Behaviour in Smartphone Interaction using Multiple Inbuilt Sensors*. arXiv preprint arXiv:2002.00918.

Adebesin, F., Kotzé, P. and Gelderblom, H., 2011. *Design research as a framework to evaluate the usability and accessibility of the digital doorway.* Design, Development & Research Conference, Cape Peninsula University of Technology, Cape Town, 26-27 September 2011. pp. 306 – 323.

Adetunji, T.O., Zuva, T. and M. and Appiah, *A.,* 2018. *Framework of Bimodal Biometrics for E-assessment Authentication Systems.* International Conference on Intelligent and Innovative Computing Applications (ICONIC), Plaine Magnien, Mauritius. 6 – 7 December. pp. 1-5.

Adil, M., Simon, R. and Khatri, S. K., 2019. *Automated Invigilation System for Detection of Suspicious Activities during Examination.* The Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, 4 – 6 February, pp. 361-366.

Agboola, O.O. and Hiatt, A.C., 2017. Delivery of summative assessment matters for improving at-risk student learning. *Journal of College Science Teaching*, 47(1), p.76.

Aggarwal, G., Ratha, N., Jea, T.Y., Bolle, R., 2008. *Gradient-based Textural Characterization of Fingerprints.* In 2008 IEEE Second International Conference on Biometrics: Theory, Applications and Systems, Arlington, Virginia, USA. 29 September – 1 October 2008. pp. 219–223.

Agrawal, V., Paliwal, R.K., Sharma, P. and Shrivastava, A., 2019. *Web Security Using User Authentication Methodologies: CAPTCHA, OTP and User Behaviour Authentication.* In Proceedings of 10th International Conference on Digital Strategies for Organizational Success. Gwalior, MP, India. 5 - 7 January 2019. pp.1578- 1589.

Agulla, Rifón, L.A., Castro, J.L.A. and Mateo, C.G. 2008, July. *Is my student at the other side? Applying biometric web authentication to e-learning environments.* In 2008 Eighth IEEE International Conference on Advanced Learning Technologies (ICALT 2008). IEEE Computer Society. Santander, Cantabria, Spain. pp. 551-553.

Ahmed, A.A.E. and Traore, I., 2007. *A new biometric technology based on mouse dynamics.* IEEE Transactions on dependable and secure computing, 4(3), pp.165-179.

Ajjawi, R., Tai, J., Dawson, P. and Boud, D., 2018. *Conceptualising evaluative judgement for sustainable assessment in higher education*. In Developing Evaluative Judgement in Higher Education (pp. 23-33). Routledge Publishing.

Akintunde, O.O. and Selzing-Musa, G., 2016. *Pragmatic Techniques of Curbing Examination Malpractices in Secondary Schools in Nigeria.* Asia Pacific Journal of Education, Arts and Sciences, 3(1). pp: 110- 115.

Alammary, A., 2019. *Blended learning models for introductory programming courses: A systematic review.* PloS one, 14(9), p. e0221765.

Allen, I. E., & Seaman, J. (2013). *Changing course: Ten years of tracing online education in the United States*. San Francisco, CA: Babson Survey Research Group and Quahog Research Group LLC.

Almalki S., Chatterjee P., Roy K. 2019. *Continuous Authentication Using Mouse Clickstream Data Analysis*. In: Wang G., Feng J., Bhuiyan M., Lu R. (eds) Security, Privacy, and Anonymity in Computation, Communication, and Storage. SpaCCS 2019. Lecture Notes in Computer Science, vol 11637. Springer, Cham, Switzerland.

Alotaibi, S. 2010. *Using biometrics authentication via fingerprint recognition in e-Exams in e-Learning environment.* Thesis (Masters). The 4th Saudi International Conference, The University of Manchester, UK. 29 - 30 Jul 2010.

Alruwais, N., Wills, G., & Wald, M., 2018. *Advantages and challenges of using e-assessment*. International Journal of Information and Education Technology, 8(1), pp. 34 – 37.

Al-Saleem, S.M. and Ullah, H., 2014. Security considerations and recommendations in computer-based testing. *The Scientific World Journal*, (1) 2014, pp. 28 – 35.

Ambler, S.W., 2005. *Feature driven development (FDD) and agile modelling*. Agile Modelling 2005(1).

Anderson, C. and Gades, P., 2017. *Proctoring exams in an online environment.* Innovate! Teaching with Technology Conference 2017. 13 – 14 June 2017. University of Minnesota Morris, Morris, Minnesota. pp. 98 -106.

Andrejevic, M. and Selwyn, N., 2020. *Facial recognition technology in schools: critical questions and concerns*. Learning, Media and Technology, 45(2), pp.115-128.

Anima, B.A., Jasim, M., Rahman, K.A. and Hasanuzzaman, M., 2016, December. *User authentication based on mouse movement data using normalized features.* In 2016 19th International Conference on Computer and Information Technology (ICCIT). USA. pp. 399-404. IEEE.

Apampa, KM, Wills, GB & Argles, D. 2009.*Towards Security Goals in Summative E-Assessment Security.* Proceedings of the ICITST 2009 Conference, United Kingdom. 09 - 12 Nov 2009.

Apampa, K.M. 2010. *Presence verification for summative e-assessments*. University of Southampton, School of Electronics and Computer Science, Thesis (Doctoral).

Araújo, L.C., Sucupira, L.H., Lizarraga, M.G., Ling, L.L. and Yabu-Uti, J.B.T., 2005. *User authentication through typing biometrics features.* IEEE transactions on signal processing, 53(2), pp.851-855.

Arnautovski, L., 2019. *Face recognition technology in the exam identity authentication system-implementation concept*. Proceedings of Papers, p.50.

Asha, S., Chellappan, C., 2008, April. *Authentication of e-learners using multimodal biometric technology*. In 2008 International Symposium on Biometrics and Security Technologies. Islamabad, Pakistan. 23-24 April 2008. pp. 1-6. IEEE.

AV, S.K. and Rathi, M., 2019. *Keystroke Dynamics: A Behavioural Biometric Model for User Authentication in Online Exams*. In Biometric Authentication in Online Learning Environments (pp. 183-207). IGI Global.

Bailie, J.L., & Jortberg, M.A. (2009). Online learner authentication: verifying the identity of online users. *Journal of Online Learning and Teaching*, 5(2), 197-207.

Bal, A. and Acharya, A., 2011. December. *Biometric authentication and tracking system for online examination system*. In 2011 International Conference on Recent Trends in Information Systems. 21 - Dec 23, 2011. Jadavpur University, Kolkata. India. pp. 209-213. IEEE.

Baleni, Z.G., 2015. Online formative assessment in higher education: Its pros and cons. *Electronic Journal of e-Learning*, 13(4), pp.228-236.

Barclay, A. and Yagolnitzer. L. 2011. *Online Student Validation*. Mathematics and Computer Science Capstones. 4. Accessed from http://digitalcommons.lasalle.edu/mathcompcapstones/4 Retrieved on 9 June 2019.

Bass, L., Clements, P. and Kazman, R., 2013. *Software Architecture in Practice*, 3rd edition. Addison Wesley.

Batyuk, A. and Verhun, V., 2018, August. *Software architecture design of the real-time processes monitoring platform*. In 2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP) (pp. 98-101). IEEE.

Beaudin, S. 2016. *An Empirical Study of Authentication Methods to Secure E-learning System Activities Against Impersonation Fraud*. Dissertation (Doctoral). Nova South-eastern University. Accessed from NSUWorks, College of Engineering and Computing. (958) at http://nsuworks.nova.edu/gscis_etd/958 Retrieved on 12 July 2018.

Bedford, W., Gregg, J., & Clinton, S., 2011. *Preventing Online Cheating with Technology: A Pilot Study of Remote Proctor and an Update on Its Use*. Journal of Higher Education Theory and Practice, 11(2), 41-58.

Begum, A. and Raj, V.C., 2018. Architectural analysis for mobile devices with quality attributes using architecture trade-off analysis method. *Journal of Computational and Theoretical Nanoscience*, 15(11-12), pp.3352-3358.

Bell, B. S., & Fedeman, J. E. (2013). *E-learning in postsecondary education*. The Future of Children, 23(1), 165-185.

Belotto, M.J., 2018. *Data analysis methods for qualitative research: Managing the challenges of coding, interrater reliability, and thematic analysis*. The Qualitative Report, 23(11), pp.2622-2633.

Benoot, C., Hannes, K. and Bilsen, J., 2016. *The use of purposeful sampling in a qualitative evidence synthesis: A worked example on sexual adjustment to a cancer trajectory*. BMC medical research methodology, 16(1), p.21.

Bhagat, V. and Katankar, V., 2014. Novel method for student authentication in online examination. *International Journal of Research*, 1(7), pp.974-979.

Bhattacherjee, A. and Barfar, A., 2011. Information technology continuance research: current state and future directions. *Asia Pacific Journal of Information Systems*, 21(2), pp.1-18.

Biggio, B. and Roli, F., 2018. *Wild patterns: Ten years after the rise of adversarial machine learning.* Pattern Recognition, 84, pp.317-331.

Black, P., 2015. *Formative assessment – an optimistic but incomplete vision.* Assessment in Education: Principles, Policy & Practice, 22(1), pp.161-177.

Blau, I., & Eshet-Alkalai, Y., (2016). *Cheating through digital technologies from perspectives of Israeli students, teachers and parents – Patterns and coping strategies.* Research report for Chief Scientist Foundation, Ministry of Higher Education.

Bohnsack, R. and Margolina, A., 2019. Teaching business models via blended learning. *Journal of Business Models*, 7(3), pp.24-37.

Bokhove, C. and Downey, C., 2018. *Automated generation of 'good enough' transcripts as a first step to transcription of audio-recorded data*. Methodological Innovations, 11(2), pp.2 – 10.

Bolin, A. 2004. Self-control, perceived opportunity, and attitudes as predictors of academic dishonesty. *Journal of Psychology*, 138(2), 101-114.

Boucké, N., Weyns, D., Schelfthout, K. and Holvoet, T., 2006, June. *Applying the ATAM to an architecture for decentralized control of a transportation system*. In International Conference on the Quality of Software Architectures (pp. 180-198). Springer, Berlin, Heidelberg.

Bowen, G.A., 2009. *Document analysis as a qualitative research method*. Qualitative Research Journal, 9(2), pp.27-40.

Bowness, P., EMC Corp, 2016. *Automated token renewal using OTP-based authentication codes*. U.S. Patent 9, 432, 339.

Braun, V., Clarke, V., Hayfield, N. and Terry, G., 2018. *Thematic analysis*. Handbook of research methods in health social sciences, pp.1-18.

Bretag, T., Harper, R., Burton, M., Ellis, C., Newton, P., van Haeringen, K., Saddiqui, S. and Rozenberg, P., 2019. *Contract cheating and assessment design: exploring the relationship.* Assessment & Evaluation in Higher Education, 44(5), pp.676-691.

Brimble, M., (2016). *Why students cheat: An exploration of the motivators of student academic dishonesty in Higher Education*. In T. Bretag (Ed.). Handbook of academic integrity. pp. 365-382. Springer-Nature: Springer Science-Business Media Singapore.

Bruno, E.P. & Aparecido N.M. 2009. *A Video-Based Biometric Authentication for e-Learning Web Applications*. Enterprise Information Systems. Lecture Notes in Business Information Processing, 24(IV): 770-779.

Bruno, U and Ibidigbo, G (2012) The counselling implications of examination malpractices among university undergraduates. *Research Journal of Organizational Psychology and Educational Studies*,1 (2), 199 – 202.

Budgen, D. *Software Design.* 2nd Edition. 2003. Addison Wesley. pp. 79 – 81.

Busayo, I (2008*) Library Intervention Strategies against Examination Malpractices in Tertiary Education Institution*. In Achebe, N (ed). Library and Information Literacy for Higher Education. Enugu, Nigeria: Nigeria Library Association.

Capilla, R., Jansen, A., Tang, A., Avgeriou, P. and Babar, M.A., 2016. 10 years of software architecture knowledge management: practice and future. *Journal of Systems and Software*, 116, pp.191-205.

Cartes, A.C., Frantz, C.J. and Reed, M.B., *System and Method for remote management of a computer.* Hewlett Packard Enterprise Development LP, 2017. U.S. Patent 9,608,884.

Castella-Roca, J., Herrera-Joancomarti, J. and Dorca-Josa, A., 2006. *A secure e-exam management system*. In First International Conference on Availability, Reliability and Security *(ARES'06).* Vienna, Austria. 20 – 26 April. IEEE Computer Society. pp. 864 - 871.

Chen, A. and Karahanna, E., 2018. *Life interrupted: The effects of technology-mediated work interruptions on work and nonwork outcomes*. MIS Quarterly, 42(4), pp.1023-1042.

Chua, S.S., Bondad, J.B., Lumapas, Z.R. and Garcia, J.D., 2019. *Online Examination System with Cheating Prevention Using Question Bank Randomization and Tab Locking.* In 2019, 4th International Conference on Information Technology (InCIT). 24-25 October 2019, Bangkok, Thailand. 24 - 25 October 2019. pp. 126-131. IEEE Computer Society.

Chuang, C.Y., Craig, S.D. and Femiani, J., 2017. *Detecting probable cheating during online assessment based on time delay and head pose*. Research & Development, 36, (6), pp. 1123-1137.

Cluskey, J, Ehlen, C R & Raiborn, MH. 2011. Thwarting online exam cheating without proctor supervision. *Journal of Academic and Business Ethics*, 4, 1–7.

Colquitt, D. and Leaney, J., 2007. *Expanding the view on Complexity within the Architecture Trade-off Analysis Method.* In 14th Annual IEEE International Conference and Workshops on the Engineering of Computer-Based Systems (ECBS'07). Tucson, Arizona, USA. 26-29 March 200. pp. 45-54. IEEE Computer Society.

Counsell, C. *Formulating questions and locating primary studies for inclusion in systematic reviews*. Annals of Internal Medicine. 1997 (127):380 – 387.

Cronan, T.P., McHaney, R., Douglas, D.E. and Mullins, J.K., 2017. *Changing the academic integrity climate on campus using a technology-based intervention.* Ethics & Behaviour, 27(2), pp. 10-15.

Cross, N. (Ed.), 1984. *Development of Design Methodology*. Wiley.

Curdt-Christiansen, X.L., 2019. *Observations and field notes: Recording lived experiences*. In the Routledge Handbook of Research Methods in Applied Linguistics. pp. 336 - 347. Routledge.

Dagilyte, E. and Coe, P., 2019. *Take-home exams: Developing professionalism via assessment*. Perspectives on the Scholarship of Assessment and Learning in Law. Australian National University Press. p.p. 109 - 166.

Daumiller, M. and Janke, S., 2019. *The impact of performance goals on cheating depends on how performance is evaluated.* AERA Open, 5(4), p.2332858419894576.

De la Orden, A., 2011. *Reflections on competency-based assessment in education*. Revista Electrónica de Investigación Educativa, 13(2), pp.1-21.

Denscombe, M. 2004. *Ground Rules for Good Research. Part One, 'Foundations for Social Research'*. Maidenhead: Open University Press.

Deranek, J. and Parnther, C., 2015. *Academic honesty and the new technological frontier*. The Hilltop Review, 8(1), p.4.

Diego, L.A.B., 2017. Friends with benefits: causes and effects of learners' cheating practices during examination. *IAFOR Journal of Education*, 5(2), pp.121-138.

Draaijer, S., Jefferies, A. and Somers, G., 2017, October. Online proctoring for remote examination: a state of play in higher education in the EU. In International Conference on Technology Enhanced Assessment. 5 – 6 October. Barcelona, Spain. pp. 96 - 108. Springer, Cham.

Dudovskiy, J., 2016. *The ultimate guide to writing a dissertation in business studies: A step-by-step assistance*. Pittsburgh, USA.

Dunn, T.P., Meine, M.F., & McCarley, J., 2010. The remote proctor: an innovative technological solution for online course integrity. *The International Journal of Technology, Knowledge and Society*, 6(1), 1-7.

Eckles, B.T. 2010. *A study of faculty and academic administrators' perceptions of academic dishonesty in Higher education in relation to learning organization for which they work* (Doctoral dissertation) pp. 2 – 3.

Eric, F & Kazimierz, K. 2010. *Continuous Biometric User Authentication in Online Examinations*. Proceedings of the Seventh International Conference on Information Technology. Las Vegas, Nevada, USA, 12-14 April 2010. pp.488-492.

Etikan, I., Alkassim, R. and Abubakar, S., 2016. Comparison of snowball sampling and sequential sampling technique. *Biometrics & Biostatistics International Journal*, 3(1), pp.1-9.

Examination Malpractice Act (2012) *'Examination Malpractice: Meaning'.* Accessed from http://ozelacademy.com/EJESV1N3_1.pdf_br Retrieved on October 6, 2018.

Fask, A., Englander, F. & Wang, Z. 2014., Do online exams facilitate cheating? an experiment designed to separate possible cheating from the effect of the online test taking environment. *Journal of Academic Ethics* 12, pp.101–112 (2014).

Fayyoumi A., Zarrad, A (2014) *Novel solution based on face recognition to address identity theft and cheating in online examination systems*. Advances of Internet Things 4(1), pp. 5 – 12.

Fenu, G., Marras, M. and Boratto, L., 2018. *A multi-biometric system for continuous student authentication in e-learning platforms.* Pattern Recognition Letters, 113, pp.83-92.

Fisher, E., McLeod, AJ, Savage A & Simkin, MG. 2016. Ghost-writers in the cloud. *Journal of Accounting Education*. pp. 34: 59.

Flick, U. 2009. An introduction to qualitative research (4th Edition). London; Sage. Pp. 5 -6.

Flior, Eric, and Kazimierz Kowalski. *Continuous biometric user authentication in online examinations.* In 2010 Seventh International Conference on Information Technology: New Generations. Las Vegas, Nevada, USA, 12-14 April 2010. pp. 488-492. IEEE Computer Society.

Foster, D. and Layman, H., 2013. Online proctoring systems compared. *Webinar. http://www. slideshare.net/caveonweb/caveon-webinar-series-online-proctoring-best-practicesoct-2013-slideshare-final*.

Friedman, A., Blau, I. and Eshet-Alkalai, Y., 2016. Cheating and feeling honest: committing and punishing analogue versus digital academic dishonesty behaviours in higher education. *Interdisciplinary Journal of E-Learning & Learning Objects*, 12(1).

Fung, C., Blue Goji Corp, 2017. *Incorporating biometric data from multiple sources to augment real-time electronic interaction*. U.S. Patent Application 14/920,831.

Gacek, C., Abd-Allah, Clark, B., Boehm, B. 1995. On the definition of software system architecture, In Proc. of 1st International Workshop on Architectures for Software Systems – In Cooperation with the 17th International Conference on Software Engineering, 1995.

Galiyawala, H.J. and Chaudhari, R., 2019. *Hand Geometry-and Palmprint-Based Biometric System with Image Deblurring*. In Information and Communication Technology for Competitive Strategies pp. 591-604. Springer, Singapore.

Gama, K. 2017. *Preliminary findings on software engineering practices in civic hackathons*. In 2017 IEEE/ACM 4th International Workshop on Crowdsourcing in Software Engineering (CSI-SE) pp. 14 – 20. IEEE, 2017.

Gao, Q., 2012. Biometric authentication to prevent e-cheating. *Instructional Technology Journal* Vol. 3(1). pp. 3 – 13.

Gathuri, J.W., Luvanda, A., Matende, S. and Kamundi, S., 2014. Impersonation challenges associated with e-assessment of university students. *Journal of Information Engineering and Applications*, 4(7), pp.60-68.

Goodman-Deane, J., Mieczakowski, A., Johnson, D., Goldhaber, T. and Clarkson, P.J., 2016. *The impact of communication technologies on life and relationship satisfaction*. Computers in Human Behaviour, 57, pp. 219 - 229.

Grijalva, TC, Nowell, C & Kerkvliet, J. 2010. Academic honesty and online courses. *College Student Journal*, 40(1), p. 180.

Grunin, G., Nassar, N.M. and Nassar, T.M., International Business Machines Corp, 2019. *System, method and computer program product for generating a cognitive one-time password.* U.S. Patent 10,389,707.

Gupta, S.G.D.M., 2017. A study of attitude of teachers and students towards open book and closed book assessment. *International Journal of Scientific Research and Management*, 5(7), pp.6034-6038.

Gustavii, B., 2012. *How to prepare a scientific doctoral dissertation based on research articles*. Cambridge University Press.

Hall, L. 2001. *take-home tests: educational fast food for the new millennium*. *Journal of Management & Organization, 7(2), 50–57.*

Hamilton, I.R.A., O'Connell, B.M., Pavesi, J.R. and Walker, K.R., *Authentication based on previous authentications*. International Business Machines Corp, 2017. U.S. Patent 9,686,262.

Harbin, J.L. and Humphrey, P., 2013. Online cheating-the case of the emperor's clothing, elephant in the room, and the 800 lb. gorilla. *Journal of Academic and Business Ethics,* 7, pp.1 - 7.

Hart, L., Morgan, L., 2010. Academic integrity in online registered nurse to baccalaureate in nursing program. *Journal of Continuing Education in Nursing*, 41 (11), 498-5-5.

Hasselbring, W., 2018. *Software architecture: Past, present, future.* In The Essence of Software Engineering. Springer, Cham, Switzerland. pp. 169-184.

Hayashi D, Akakura T. 2018. *Proposal for Writing Authentication Method Using Tablet PC and Online Information in e-Testing*. In International Conference on Human Interface and the Management of Information. Springer, Cham, Switzerland. pp 253-265.

Hayes B, Ringwood, J. 2009. *Authenticating student work in eLearning programme via speaker recognition*, Proceedings of the 3rd international conference on signals, circuits and systems (SCS) 2009, 6-8 November. Djerba, Tunisia. IEEE Computer Society.

Hayford, E., Lang, JM. 2013. Cheating lessons: learning from academic dishonesty. *Library Journal,* 138(16), p. 82.

Hay-Gibson, N.V., 2009. *Interviews via VoIP: Benefits and disadvantages within a PhD study of SMEs.* Thesis (Doctoral). Library and Information Research, 33(105), pp.39-50.

Heckler, N.C., Rice, M., and Bryan, C.H. (2013). *Journal of Research on Technology in Education*, 45(3), 229- 248.

Hedaia, O.A., Shawish, A., Houssein, E.H. and Zayed, H., 2020. Bio-CAPTCHA voice-based authentication technique for better security and usability in cloud computing. *International Journal of Service Science, Management, Engineering, and Technology (IJSSMET)*, 11(2), pp.59-79.

Hernandez, JA., Ortiz, AO., Andaverde, J & Burlak, G. 2008. *Biometrics in Online Assessments: A Study Case in High School Students*. Retrieved from https://www.researchgate.net/publication/4324405_Biometrics_in_Online_Assessments_A_Study_Case_in_High_School_Students. [12 August 2018]

Hervatis, V., Kyaw, B.M., Semwal, M., Dunleavy, G., Car, L.T., Zary, N. and Car, J., 2016. *Offline and computer-based eLearning interventions for medical students' education*. Cochrane Database of Systematic Reviews, (4).

Hevner, A., Chatterjee, S. 2010. *Design Research in Information Systems*. In Design Research in Information Systems, Integrated Series in Information Systems 22. 9–22. Retrieved from http://link.springer.com/10.1007/978-1-4419-5653-8. [20 August 2018].

Hilliard, R., 2007. All About IEEE Std 1471. *IEEE Recommended Practice for Architectural Description of Software Intensive Systems* (IEEE Std 1471-2000).

Hinman, L. M., (2000). *Academic integrity and the World Wide Web*. ACM SIGCAS Computers and Society, 2002 pp. 3 – 4.

Hofmeister, C., Nord, VL., Soni, D. 1999. *Describing Software architectures with the UML.* Proceedings of the First Working IFIP Conference on Software Architecture. 22–24 February 1999, San Antonio, Texas, USA. pp. 1 – 4.

Holden, M. and Mettyear, N., Wacom Co Ltd, 2018. *Dynamic handwriting verification, handwriting-based user authentication, handwriting data generation, and handwriting data preservation*. U.S. Patent 10,032,065.

Hollister, K.K. and Berenson, M.L., 2009. Proctored versus unproctored online exams: Studying the impact of exam environment on student performance. *Decision Sciences Journal of Innovative Education,* 7(1). pp.271-294.

Hovhannisyan, A., 2020. *Cheating and Plagiarism in Armenia: Why Not?* In Corruption in Higher Education. pp. 30 - 34. Brill Sense.

Huffmeyer, M., Haupt, F., Leyman, F. and Schreier, U., 2018. Authorization-aware HATEOAS. In CLOSER. pp.78 – 89.

Ismail, E.S. and Syed-Musa, S.M.S., 2018. *Timestamp-based password authentication scheme.* In AIP Conference Proceedings. Pahang, Malaysia. 5 - 6 July 2018. Vol. 1974, No. 1, p. 020051. AIP Publishing LLC.

James, C.L., 2019. *Cheating on Tests: The Adventure Continues*. In Adventures in teaching. 2019 (22). pp. 12 – 18.

James, R., 2016. Tertiary student attitudes to invigilated, online summative examinations. *International Journal of Educational Technology in Higher Education,* 13(1), p.19.

Jaswal, G., Kaul, A. and Nath, R., 2019. *Multimodal biometric authentication system using hand shape, palm print, and hand geometry.* In Computational Intelligence: Theories, Applications and Future Directions-Volume II pp. 557-570. Springer, Singapore.

Jenkins, R., White, D., Van Montfort, X. and Burton, A.M., 2011. *Variability in photos of the same face.* Cognition, 121(3), pp.313-323.

Johnson, D.R., Scheitle, C.P. and Ecklund, E.H., 2019. *Beyond the In-Person Interview: How Interview Quality Varies Across In-person, Telephone, and Skype Interviews*. Social Science Computer Review, p.0894439319893612.

Joint Information Systems Committee (JISC) (2006). *Effective Practice with online assessment*. An overview of technologies, policies and practice in further and higher education. Roadmap for online assessment Report for JISC (Open University, 2006), London UK. pp. 10-20.

Jones, I.M. (2009). *Cyber-Plagiarism: Different Method Same Song. Journal of Legal, Ethical and Regulatory Issues*, 12(1), pp. 89-100.

Jung, I.Y. and Yeom, H.Y., 2009. *Enhanced security for online exams using group cryptography.* IEEE transactions on Education, 52(3), pp.340-349.

Kanamarlapudi, S., Hsu, L., Ramalingham, S., Iyer, R.R., Sheik, A.A. and Gunasegaran, S., Qualcomm Inc., 2016. *Enhanced timer handling mechanism.* U.S. Patent 9,503,888.

Karim, M., Heickal, H. and Hasanuzzaman, M., 2017, February. *User authentication from mouse movement data using multiple classifiers*. In Proceedings of the 9th International Conference on Machine Learning and Computing. Nanning, China, July 28 – 31. pp. 122-127.

Karim, N, Shukur, AZ. 2015. Review of user authentication methods in online examinations. *Asian Journal of Information Technology* 14(5). pp. 166-175. ISSN 1682-3915.

Karim, N, Shukur, AZ. 2016. Using preferences as user identification in the online examination, *International Journal on Advanced Science Engineering Information Technology,* vol. 6, no. 6, pp. 2088-5334, 2016.

Keil, S., Brown, A. 2014. *Distance Education Policy Standards: A Review of Current Regional and National Accrediting Organizations in the United States*. *Online Journal of Distance Learning Administration,* 17(3), p15.

Kinoti, P. (2015). *Addressing Impersonation Threats in Online Assessment Environment Using Temporal Information and System Interactions*. Merit Research Journal of Education and Review. 3. pp. 215-220.

King, D.L., Case, C.J., 2014. *E-cheating: Are students misusing IT?* Issues in Information Systems, 15(1).

Kirkpatrick, K. (2015). *Technology Brings Online Education in Line with Campus Programs*. The Communications of the ACM, 58(12), 17-19.

Kishore, R., Suriya, S. and Vivek, K.V., 2019. *Enhanced Security for ATM Machine with OTP and Facial Recognition Features*. International Research Journal of Multidisciplinary Technovation, 1(2), pp.106-110.

Kitchenham, B., Pretorius, R., Budgen, D., Brereton, O.P., Turner, M., Niazi, M. and Linkman, S., 2010. *Systematic literature reviews in software engineering–a tertiary study*. Information and software technology, 52(8), pp.792-805.

Ko, CC., Cheng, CD. 2008. Flexible and secure computer-based assessments using single zip disk. *Computer Education Journal*. 50. pp. 915-926.

Kritzinger. E., von Solms, SH. 2006. E-learning: incorporating information security governance, informing science: *International Journal of an Emerging Trans discipline*, vol. 3, pp. 319-325.

Kruchten, P.B., 1995. *The 4+ 1 view model of architecture*. IEEE software, 12(6), pp.42-50.

Kruchten, P., Capilla, R. and Dueñas, J.C., 2009. *The decision view's role in software architecture practice.* IEEE software, 26(2), pp.36-42.

Lambert, S.D. and Loiselle, C.G., 2008. Combining individual interviews and focus groups to enhance data richness. *Journal of Advanced Nursing*, 62(2), pp.228-237.

Lange, C.F., Chaudron, M.R. and Muskens, J., 2006. *In practice: UML software architecture and design description*. IEEE software, 23(2), pp.40-46.

Laplante, P.A., 2017. *Requirements engineering for software and systems*. Auerbach Publications.

Lee, H.Y., Choi, J.H., Yi, N.Y., Lee, M.J., Chang, H.J., Choi, E.H., Chung, M.J., Gang, G.O., Lee, H.L., Lee, K.E. and Kwak, T.K., 2018. Development of materials for food safety and nutrition management program for single seniors with a life manager-by focus group interview and delphi technique. *Journal of The Korean Society of Food Science and Nutrition*.

Lee, J. and Kotonya, G., 2010. *Combining service-orientation with product line engineering*. IEEE software, 27(3), pp.35-41.

Lee, Y.K., Nam, D. and Medvidovic, N., 2016. *Identifying Inter-Component Communication Vulnerabilities in event-based Systems.* Technical ReportL USC-CSSE-17-801, 2016.

Lee-Post, A. & Hapke, H., (2017). *Online learning integrity approaches: Current practices and future solutions*, Online Learning 21(1),135-145.

Lemke, G. *The Software Development Life Cycle and Its Application.*2018. Senior Honours Theses & Projects. 589. Accessed from https://commons.emich.edu/honors/589. retrieved on 7 August 2019.

Leng, L., Gao, F., Chen, Q. and Kim, C., 2018. *Palmprint recognition system on mobile devices with double-line-single-point assistance*. Personal and Ubiquitous Computing, 22(1), pp.93-104.

Le Saint, E., Chen, Y., Kekicheff, M and Fredronic, D. Visa International Service Association, 2019. *Multi-level communication encryption.* US. Patent Application 16/084, 480.

Levy, Y., Ramim, MM. 2007. *A theoretical approach for biometric authentication of eExams.* Proceedings of the Chais Conference on Instructional Technologies research. 20 – 22 February. Raanana Israel, pp: 93 – 101.

Li, B., Wang, W., Gao, Y., Phoha, V.V. and Jin, Z., 2018, October. *Hand in Motion: Enhanced Authentication Through Wrist and Mouse Movement*. In 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS). Los Angeles, California. 22 – 25 October. pp. 1-9. IEEE Computer Society.

Ligatti, J.A., Goldgod, D., Cetin, C. and Subils, J.B., University of South Florida, 2017. *System and Method for authentication using multiple devices. U.S. Patent 9,659,160.*

Lu H., Rose J., Liu Y., Awad A., Hou L., (2017) *Combining Mouse and Eye Movement Biometrics for User Authentication*. In: Traoré I., Awad A., Woungang I. (eds) Information Security Practices. Springer, Cham, Switzerland.

Mack, N., Woodsong, C., MacQueen, K.M, Guest, G., Namey, E. 2005. *Qualititative Research Methods: A Data Collector's Field Guide.* Family Health International, USA, USAID.

Magno, Carlo and Lizada, Gabriel Sebastian, *Features of Classroom Formative Assessment.* 2015. Educational Measurement and Evaluation Review, Vol. 6, 2015.

Mahbub, U., Sarkar, S., Patel, V.M. and Chellappa, R., 2016, September. *Active user authentication for smartphones: A challenge data set and benchmark results.* In 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS). 6 - September. Niagara Falls, Buffalo, New York (USA). pp. 1 - 8. IEEE Computer Society.

Mahesh, P. and K. Selvajyothi. *Impersonation detection in online examination.* 2017 IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES), Kollam, Kerala, India. 8 - 10 August 2017, pp. 1-5.

Mann, S., 2016. *The research interview*. *Reflective practice and reflexivity in research processes*. Springer.

Mantoro, T. and Johnson, C., 2003*. Location history in a low-cost context awareness environment*. In Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003-Volume 21. pp. 153-158. Australian Computer Society, Inc.

Marsh S (2017) *More university students are using tech to cheat in exams.* The Guardian. Retrieved at https://www.theguardian.com/education/2017/apr/10/more-university-students-are-using-tech-to-in-exams. Accessed 19 Nov 2019.

Martinez, C., 2019. *Online Exam Proctoring: Viewpoints of Military High Schools* (Doctoral dissertation). The University of Nebraska-Lincoln.

Marton G. and David A. *Security considerations and two-factor authentication opportunities in e-learning environments*. *ICETA 2014 - 12th IEEE Int. Conf. Emerg. eLearning Technol. Appl. Proc.,* pp. 319–323, 2015.

Maxwell, J.A., 2012. *Qualitative research design: An interactive approach*. Sage publications pp. 42 – 44.

Mayer, R.E., 2019. *Computer games in education*. Annual review of psychology. Vol. *70*, pp.531-549.

Mcallister, C., & Watkins, P. (2012). *Increasing Academic Integrity in Online Classes by Fostering the Development of Self-Regulated Learning Skills*. The Clearing House (85). pp. 96-101.

McCabe, DL., Treviño, LK, & Butterfield, K D. 2001. *Cheating in academic institutions: A decade of research*. Ethics and Behaviour, 11(3), pp. 219–232.

McMurtry, K., 2001. E-cheating: Combating a 21st century challenge*. The Journal of Technological Horizons in Education,* 29(4), p.36.

McNabb, L., (2010). *An Update on Student Authentication: Implementation in Context.* Continuing Higher Education Review, 74, 43-52.

Mead, N.R., Garlan, D. and Shaw, M., 2018. *Half a century of software engineering education: The CMU exemplar*. IEEE Software, 35(5), pp.25-31.

Medvidovic, N., Taylor, RN., 2010. *Software architecture: foundations, theory, and practice.* In 2010 ACM/IEEE 32nd International Conference on Software Engineering (Vol. 2, pp. 471 – 472). IEEE.

Mellar, Harvey & Peytcheva-Forsyth, Roumiana & Kocdar, Serpil & Karadeniz, Abdulkadir & Yovkova, Blagovesna. (2018). *Addressing cheating in e-assessment using student authentication and authorship checking systems: Teachers' perspectives*. International Journal for Educational Integrity. 14. 2. 10.1007/s40979-018-0025-x.

Miguel, E.M., Ruiz, M.D.C.S., Blas, E.G.C. and Perea, C.M., 2018. *Competency assessment impact in quality of learning: Nursing degree learners and teachers' perception*. Enfermería Global, (50), p.420.

Mitchel, M. L., & Jolley, J. M. (2013). *Research design explained*. California: Cengage Learning.

Moini A., Madni AM., 2009. Leveraging biometrics for user authentication in online learning: a systems perspective, *IEEE Systems Journal*, vol. 3, no. 4. pp. 35 – 42.

Molten Jr, J., Fitterer, A., Brazier, E., Leonard, J., & Brown, A., 2013. Examining online college cyber cheating methods and prevention measures. *The Electronic Journal of e-Learning*, Vol. 11, Issue 2, 139-146.

Monrose, F. & Rubin, AD. 2000. *Keystroke dynamics as a biometric for authentication.* Future Generation Computer Systems, vol. 16, no. 4, pp. 351–359.

Montenegro, C.H., Astudillo, H. and Álvarez, M.C.G., 2017, September. *ATAM-RPG: A role-playing game to teach architecture trade-off analysis method (ATAM)*. In 2017 XLIII Latin American Computer Conference (CLEI). 4th-8th September 2017, Córdoba, Argentina. pp. 1-9. IEEE.

Moore, M., & Kearsley, G., (2012). *Distance education: A systems view of online learning* (3rd ed.). Belmont, CA: Wadsworth. Parker, K., Lenhart, A., & Moore, K. 2011. The digital revolution and higher education: College presidents, public differ on value of online learning. Washington D.C.: Pew Research Centre.

Moten, A.R., 2014. *Academic dishonesty and misconduct: Curbing plagiarism in the Muslim world*. Intellectual Discourse, 22(2) p. 38.

Mungai, P.K. and Huang, R., 2017, March. *Using keystroke dynamics in a multi-level architecture to protect online examinations from impersonation*. In 2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA). pp. 622-627. IEEE.

Muukkonen, H., Lakkala, M., Toom, A. and Ilomäki, L., 2017. *Assessment of competences in knowledge work and object-bound collaboration during higher education courses*. Higher education transitions: Theory and research, pp.288-305.

Narayanan, H., Radhakrishnan, V. and Poroor, J., 2017, March. *Architectural design for a secure Linux operating system.* In 2017 International Conference on Wireless Communication, Signal Processing and Networking (WiSPNET). 22-24 March. Chennai, India. pp. 949 – 953. IEEE Computer Society.

Nawaz, Z., Aftab, S. and Anwer, F., 2017. Simplified FDD Process Model*. International Journal of Modern Education and Computer Science*, 9(9), p.53.

Niinuma, K. and Jain, A.K., 2010, April. *Continuous user authentication using temporal information*. In Biometric Technology for Human Identification VII (Vol. 7667, p. 76670L). International Society for Optics and Photonics.

O'Gorman, L. 2003. *Comparing passwords, tokens, and biometrics for user authentication*, in Proceedings of the IEEE, vol. 91, issue no. 12, pp. 2021-2040.

Oates, B. (2006). *Researching information systems and computing*. SAGE Publications London. pp. 102 -104.

Okada, A., Whitelock, D., Holmes, W. and Edwards, C., 2019. e‐Authentication for online assessment: A mixed‐method study. *British Journal of Educational Technology*, 50(2), pp.861-875.

Olusola, O.I. and Ajayi, O.S., 2015. Moral intelligence: An antidote to examination malpractices in Nigerian schools. *Universal Journal of Educational Research*, 3(2), pp.32-38.

Omolara, A.E., Jantan, A., Abiodun, O.I., Arshad, H. and Mohamed, N.A., 2019. Fingereye: improvising security and optimizing ATM transaction time based on iris-scan authentication. *International Journal of Electrical & Computer Engineering* (2088-8708), 9(3).

Onyema, E.M., Eucheria, A.U., David, N.A., Omar, A.I.A. and Alsayed, QN.N., 2019. *The role of technology in Mitigation of Examination Malpractices in West Africa.* Sexual Abuse, 7(10). pp. 3990-4002.

Onyibe, C.O., Uma, U.U. and Ibina, E., 2015. Examination malpractice in Nigeria: causes and effects on national development. *Journal of Education and Practice*, 6(26), pp.12-17.

Oreilly, G. and Creagh, J., 2016, April. *A categorization of online proctoring*. In Global Learn (pp. 542-552). Association for the Advancement of Computing in Education (AACE).

Orlov, S. Vishnyakov, A. 2017. Decision making for the software architecture structure based in criteria importance theory. Procedia computer science, 104, pp. 27- 34.

Ouhbi, S., 2018, March. *Software Architecture Evaluation: A Systematic Mapping Study*. In ENASE pp. 447-454.

Owusu-Boampong A., Holmberg C., (2015). *Distance education in European higher education-the potential*. Report 3 (of 3) of the IDEAL (impact of distance education on adult learning).

Oxford Living Dictionary of English Online. 2018. *Oxford Press.* Retrieved from: https://www.oed.com/public/freeoed

Page, T., 2008. Ensuring software quality in engineering environments. *i-Manager's Journal on Software Engineering,* 2(4), p.1.

Palinkas, L.A., Horwitz, S.M., Green, C.A., Wisdom, J.P., Duan, N. and Hoagwood, K., 2015. *Purposeful sampling for qualitative data collection and analysis in mixed method implementation research*. Administration and policy in mental health and mental health services research, 42(5), pp.533-544.

Patnaude, KA. 2008. *Faculty perceptions regarding the extent to which the online course environment affects academic honesty* (Doctoral dissertation). University of Houston, Houston, TX.

Patra, K., Nemade, B., Mishra, D.P. and Satapathy, P.P., 2016. *Cued-click point graphical password using circular tolerance to increase password space and persuasive features*. Procedia Computer Science, 79, pp.561-568.

Perry, D.E., Wolf, A.L.1992. *Foundations for the study of software architecture*. Software Engineering Notes. Vol. 17. No 4.pp. 40 – 52.

Peytcheva-Forsyth, R. and Aleksieva, L., 2019, March. *Students' authentication and authorship checking system as a factor affecting students' trust in online assessment*. In Proceedings from INTED2019: 13th annual international technology, education and development conference, Valencia, Spain. 11 – 13 March. pp. 11-13.

Pillsbury, C. 2004. Reflections on academic misconduct: An investigating officer's experiences and ethics supplements, *Journal of American Academy of Business*, 5(1/2), pp. 446-454.

Pope, Z. and Gao, Z., 2017. *7 Global Positioning systems and geographical information systems and physical activity*. Technology in Physical Activity and Health promotion, p. 129.

Preston, C.C., & Colman, A.M. *Optimal number of response categories in rating scales: reliability, validity, discriminating power, and respondent preferences*. Acta psychologica 104, no. 1 (2000): 1 – 15.

Prince, D., Fulton, R & Garsombke, T. 2009. Comparisons of proctored versus non-proctored testing strategies in graduate distance education curriculum. *Journal of College Teaching & Learning*, 6(7), 51–62.

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

Quinlan, C., Babin, B., Carr, J. and Griffin, M., 2019. *Business research methods*. South Western Cengage.pp. 85 – 93.

Rabuzin, K., Baca, M. and Sajko, M., 2006, August. *E-learning: Biometrics as a Security Factor. In 2006 International Multi-Conference on Computing in the Global Information Technology-* (ICCGI'06). Bucharest, Romania. 1 - 3 Aug. pp. 64-64. IEEE Computer Society.

Ramu T., Arivoli, T., 2013. *A framework of secure biometric based online exam authentication: An alternative to traditional exam*. International Journal of Scientific & Engineering Research, Vol. 4, Issue 11, 2013. ISSN 2229-5518.

Rao, NSS., Harshita, P., Dedeepya, S & Uhashree, P. 2011. *Cryptography analysis of enhanced approach for secure online exam process plan*. Proceeding of the International Conference Computer Science Telecommunications. Ayia Napa, Cyprus. 8 – 11 May. vol 2 pp. 52 – 57.

Raud, Z. and Vodovozov, V., 2019, October*. Advancements and Restrictions of E-Assessment in View of Remote Learning in Engineering*. In 2019 IEEE 60th International Scientific Conference on Power and Electrical Engineering of Riga Technical University (RTUCON. Warsaw University of Technology, Poland. 07 - 09 October. pp. 1 - 6. IEEE Computer Society.

Raul, N., Shankarmani, R. and Joshi, P., 2020. *A Comprehensive Review of Keystroke Dynamics-Based Authentication Mechanism*. In International Conference on Innovative Computing and Communications. Queensland: Springer-Verlag, Singapore. pp. 149-162.

Roach, R. 2001. *Safeguarding Against Online Cheating. Black Issues in Higher Education.* Academic OneFile p. 92.

Roberts, R. and Page, M., 2019. *Secure voice biometric authentication*. U.S. Patent Application 16/164,434.

Rodchua, S., Yiadom-Boakye, G., Woolsey, R. 2011. Student verification system for online assessments: Bolstering quality and integrity of distance learning. *Journal of Industrial Technology,* vol. 27, no. 3, pp. 1-8, 2011.

Rosenberg MJ. 2011. *E-learning strategies for delivering knowledge in the digital age*, p.36. New York: McGraw Hill.

Rowe, N. 2004. Cheating in online student assessment beyond plagiarism. *Online Journal of Distance Learning Administration,* 7(2) p. 60.

Rozycki, EG. 2006. *Cheating impossible: Transforming educational values.* Educational Horizons, 84(3), pp. 136-138.

Rudrapal, D., Das, S., Debbarma, S., Kar, N. & Debbammar, N., 2012. Voice *recognition and authentication as a proficient biometric tool and its application in online exam for physically* *handicapped people.* Proceeding of the International Conference Computer Applications. Linz, Austria, 11-13 July, vol 39. pp. 6-12.

Ruhode, E. 2016. *E-Government for Development:* A thematic analysis of Zimbabwe's information and communication technology policy documents. *The Electronic Journal of Information Systems in Developing Countries,* 73(7):1-15.

Ruiz JG., Mintzer MJ., Leipzig, RM. 2006. The impact of e learning in medical education*, Journal of Medicine*, 81(3), p. 207.

Sabbah, Y., Kotb, A. & Saroit, I. 2011. *An interactive and Secure Examinations Unit (ISEEU): A proposed model for proctoring online exams*. Proceedings from the 10th Roedunet Intentional Conference (RoEduNet). Bucharest, Romania. 23 – 25 June., pp. 1-5.

Saevanee, H., Clarke, N., Furnell, S. and Biscione, V., 2015*. Continuous user authentication using multimodal biometrics*. Computers & Security, 53, pp.234-246.

Saikiran, I., Simon, R., 2019. *Agile Software Development in Distributed team enhancement Techniques*. In 2019 International Conference on Intelligent Computing and Control Systems (ICCS). Madurai, India. 15 – 17 May. pp. 1147 – 1151. IEEE.

Samangouei, P., Patel, V. M. and Chellappa, R. 2015. *Attribute-based continuous user authentication on mobile devices.* 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS), Arlington, Virginia. pp. 1-8.

Sapriati, A. and Zuhairi, A., 2010. Using computer-based testing as alternative assessment method of student learning in distance education. *Turkish Online Journal of Distance Education*, 11(2), pp.161-169.

Saraç, S. and Karakelle, S., 2017. On-line and off-line assessment of metacognition. *International Electronic Journal of Elementary Education,* 4(2), pp.301-315.

Saunders, Mark N.K.; Lewis, Philip; Thornhill, Adrian and Bristow, Alexandra. 2015. *Understanding research philosophy and approaches to theory development.* In: Saunders, Mark N. K.; Lewis, Philip and Thornhill, Adrian eds. Research Methods for Business Students. Harlow: Pearson Education, pp. 122–161.

Sekaran, U. and Bougie, R., 2016. *Research methods for business: A skill building approach*. John Wiley & Sons, pp. 28 – 31.

Seo, H.J. and Wyrwas, J., Qualcomm Inc, 2019. *On-screen optical fingerprint capture for user authentication*. U.S. Patent 10,169,637.

Sewell, J.P., Frith, K.H., & Colvin, M.M. (2010). Online assessment strategies*: A Primer Journal of Online Learning and Teaching,* 6(1), 297-305.

Shaw, M., Garlan, D. 1996. *Abstractions for software architecture and tools to support them*. IEEE Transactions on Software Engineering, Special issue on Software Architecture, Vol. 21, No. 4, pp314–335.

Shaw, DC. 2004. *Academic dishonesty in traditional and online courses as self-reported by students in online courses*. Ph.D. thesis, pp. 2 – 3.

Shih, C.C. Quanta Computer Inc., 2018. *Authentication-free configuration for service controllers. U.S. Patent 9,866,548.*

Shon, P.C., 2006. *How college students cheat on in-class examinations: Creativity, strain, and techniques of innovation.* Info: Ann Arbor, MI: MPublishing, University of Michigan Library, p.1.

Shyles, L., 2002. *Authenticating, Identifying, and Monitoring Learners in the Virtual Classroom: Academic Integrity in Distance Learning.* Pp. 2 – 6.

Simonson, M. and Seepersaud, D.J., 2018. *Distance education: Definition and glossary of terms*. 4th edition (August, 2018). Information Age Publishing.

Smith, H. and Ridgway, J., 2006, June. *Another piece in the cheating jigsaw.* In 2nd JISC International Plagiarism Conference, Newcastle-upon-Tyne, UK, 19–21 June 2006. pp. 19 - 21.

Styron, J. & Styron, RA., 2010. Student cheating and alternative web-based assessment. *Journal of College Teaching & Learning,* Vol. 7, No. 5, 37-42.

Suganya, S., Muthumari, G. & Balasubramanian, G. 2016. Improving the performance of mouse dynamics-based authentication using machine learning algorithm*. International Journal of Innovation and Scientific Research;* ISSN 2351-8014 Vol. 24 No. 1 Jun. 2016, pp. 202-209.

Sun, A. and Chen, X., 2016. Online education and its effective practice: A research review. *Journal of Information Technology Education,* 15.

Sunday, E. (2014) *Stakes Heighten in Hi-Tech Examination Malpractices*. The Guardian, Thursday, September 18, pp.3 – 4.

Swart, O., 2016. *Take-home and online timed assessments at an ODL institution*. Procedia-Social and Behavioural Sciences, 228, pp.66-71.

Tikam, M.V., 2016. *ICT Integration in Education: Potential and Challenges. In Human Development and Interaction in the Age of Ubiquitous Technology*. pp. 25-47. IGI Global.

Tirumala, S. S., Ali, S. & Babu, AG. 2016. A hybrid agile model using SCRUM and feature driven development. *International Journal of Computer Applications*, vol. 156, no. 5, pp. 1–5.

Turner III, D.W., 2010. *Qualitative interview design: A practical guide for novice investigators.* The qualitative report, 15(3), pp.754-760.

Ulinskas, M., Woźniak, M. and Damaševičius, R., 2017, July. *Analysis of keystroke dynamics for fatigue recognition.* In International Conference on Computational Science and Its Applications. Trieste, Italy, July 3-6. pp. 235-247.

Ullah, A., Xiao, H., Lilley, M. & Barker, T. 2012. Using challenge questions for student authentication in online examination*. International Journal for Infonomics (IJI)*, Volume 5, Issue 3/4, p. 8.

Ullah, A., Xiao, H., Lilley, M. and Barker, T., 2014, September. *Privacy and Usability of image and text-based challenge questions authentication in online examination*. In 2014 International Conference on Education Technologies and Computers (ICETC). Lodz, Poland. September 22-24. pp. 24 – 29. IEEE.

Underwood, J. and Szabo, A., 2003. Academic offences and e‐learning: individual propensities in cheating. *British Journal of Educational Technology*, 34(4), pp.467-477.

Vaishnavi, V.K. and Kuechler, W., 2015. *Design science research methods and patterns: innovating information and communication technology*. Crc Press.

Van der Kleij, F.M., Vermeulen, J.A., Schildkamp, K. and Eggen, T.J., 2015. *Integrating data-based decision making, assessment for learning and diagnostic testing in formative assessment. Assessment in Education: Principles, Policy & Practice*, 22(3), pp.324-343.

Velasquez, Ignacio, Angelica Caro, and Alfonso Rodriguez. *Authentication schemes and methods: A systematic literature review.* Information and Software Technology 94, pp. 30- 37.

Voas, J., 2004. *Software's secret sauce: the"-ilities"[software quality].* IEEE software, 21(6), pp.14-15.

Waghid, Y. and Davids, N., 2019. On the polemic of academic integrity in higher education. *South African Journal of Higher Education*, 33(1), pp.1-5.

Wang, D., Ming, J., Chen, T., Zhang, X. and Wang, C., 2018, May. *Cracking IoT device user account via brute-force attack to SMS authentication code.* In proceedings of the first workshop on Radical and Experiential Security. Incheon, Korea. pp. 51-60.

Watson, G., Sottile, J. 2010. Cheating in the digital age: Do students cheat more in online courses? *Online Journal of Distance Learning Administration*, 8(1), np

Weber, L.J., McBee, J.K. and Krebs, J.E., 2003. *Take home tests: An experimental study. Research in Higher Education*, 18(4), pp.473-483.

Weippl, ER. 2005. *Security in E-Learning (Advances in Information Security)*. New York: Springer-Verlag PP. 12 - 14.

Wilson, A.D., Onwuegbuzie, A.J. and Manning, L.P., 2016. *Using paired depth interviews to collect qualitative data*. The Qualitative Report, 21(9), p.1549.

Wisher, R., Curnov, C., Belanich, J. (2005) *Verifying the Learner in distance learning*, 18th Annual Conference on Distance Teaching and Learning. University of Wisconsin, Madison WI, USA. pp. 1 – 3.

Wulf, C., Hasselbring, W., Ohlemecher, J. 2017, April. *Parallel and generic pipe - and filter architectures with TeeTime*. In 2017 IEEE International Conference on Software Architecture Workshops (ICSAW). Gothenburg, Sweden.5 – 7 April. pp. 290-293. IEEE.

Xiao, Q., Yang, XD. 2009. *A facial presence monitoring system for information security.* Proceedings of the IEEE Workshop on Computational Intelligence in Biometrics: theory, Algorithms, and Applications. Nashville, Tennessee, USA, pp. 69-76.

Zheng Q., Li R., Dong B. (2019) *Using Face Recognition to Detect “Ghost Writer” Cheating in Examination*. In: El Rhalibi A., Pan Z., Jin H., Ding D., Navarro-Newball A., Wang Y. (eds) E-Learning and Games. Edutainment 2018. Lecture Notes in Computer Science, vol 11462. Springer, Cham, Switzerland.

Zhu, H., *2005. Software Design Methodology: From Principles to architectural Styles.* Elsevier.

Zviran, M, Erlich, Z. 2006. *Identification and Authentication: Technology and Implementation Issues*, Communications of the Association for Information Systems (17) Article 4, p.4.

LIST OF FIGURES

LIST OF TABLES

APPENDICES

APPENDIX A: STAKEHOLDER INTERVIEW QUESTIONS AND CONCERNS

A1 Interview questions for the students' stakeholder group

1. How old are you?
2. Would you prefer to have your parent present when we conduct the final interview?
3. What is your understanding / experience with online assessments?
4. What conditions would you expect an online assessment to satisfy in order for it to be considered "ideal" from a student's perspective?
5. How are you required to identify yourself in the online assessments that you will take / have taken?
6. Do you think that impersonation (explained) can happen in such an online assessment setting?
7. If yes, how do you think impersonation can happen in an online assessment?
8. If no, is it not possible for... (Scenario…)?
9. In what way can the system protect honest students from impersonators?
10. Would those actions not cause discomfort or disturbance?

A2 Concerns of the student stakeholder group

i. What does the system aim to achieve?

ii. Will the system work for International Certification (CompTIA, Microsoft and Oracle), Occupational Certificate, and college diploma online assessments?

iii. Can a student attempt online assessments from any place and at any time?

iv. Will the system allow the uploading of work files or quizzes to the Learning Management System?

v. How effectively can the system fight impersonation for example, students assisting each other by sharing answers, system credentials and swapping seats / places in the assessment?

vi. Will students need to take summative assessments from designated centres under invigilation?

vii. Does a student still need to make a booking prior to appearing for assessment?

viii. What proof of identity is required to access the system?

ix. How will the system verify students in routine, formative assessments? Anyone can do the work for or help the students and submit in the students' account.

x. How exactly will the system secure student's personal data?

xi. How effectively can the system "see and confirm" that the student taking the assessment is the correct student? How does the system guarantee student security and privacy?

xii. How accurate is the authentication method?

xiii. Will assessment be transparent?

xiv. How available and cheap are the technologies used in the system?

xv. Will extra authentication not be cumbersome on the student? The assessment itself may be strenuous.

xvi. Will the system be fair on all students i.e. will all students be authenticated the same way?

xvii. Will the system recognize that not all students are cheats?

A3 Interview questions for the parent's / guardians stakeholder group

1. What does the system aim to achieve?
2. How many of your children / wards engaged in online education?
3. What is your understanding / experience with online education and assessments?
4. How do you view online assessments and qualifications?
5. Do you think that students must be free to take online assessments from any place of their choosing?
6. What is your view of people cheating in online assessments?
7. Do you think that impersonation (explained) can happen in an online assessment?
8. What would you say are the effects of impersonation on education and qualifications?
9. If yes, how do you think impersonation can happen in an online assessment?
10. If no, is it not possible for... (Scenario…) **a scenario created based on previous responses for clarity.
11. In what way would you expect an online assessment system to fight impersonation?
12. How would you measure the efficiency of an assessment system against impersonation?
13. What changes would you expect those measures to have on the online assessment experience of the assessed student?
14. Would a system that implements those measures convince you to give a higher rating to online assessments or qualifications?

A4 Concerns of the parents' / guardians stakeholder group

i. Students should presently only take summative assessments from designated centres under invigilation. The young generation is computer savvy. For fairness, will the system provide invigilation?

ii. Does the authentication mechanism not invade student's privacy?

iii. Will the assessment system not hinder the student's progress through the assessment?

iv. Can parents be more involved? It would be good for students to take assessments in environments where they are most comfortable such as their homes but under supervision from parents / another adult.

v. Will the verification and authentication processes not disrupt student focus during the assessment?

vi. Will the continuous authentication systems not intimidate the student? Can the process take place in the background but with the student's knowledge?

vii. How will the system block parents and guardians from assisting the student?

viii. Can a method such as a video camera be included to ensure that the student taking the assessment is the correct student?

ix. Will the authentication process use basic hardware to keep costs of course low?

x. Will the student get a chance to familiarize with the system before the actual final assessment?

xi. Will the system not intimidate or disturb the student during the assessment?

xii. How can the student and family's privacy to be preserved?

xiii. Will the system be fair on all students?

A5 Interview questions for the faculty / stakeholder group

1. What is your understanding / experience with online assessments?
2. What conditions would you expect an online assessment to satisfy in order for it to be considered "ideal" from an educator or faculty perspective?
3. How does the online assessment system that you have worked with identify students?
4. Do you think that impersonation can happen in such an online assessment setting?
5. If yes, how do you think impersonation can happen in an online assessment?
6. What characteristics of an assessment system do you evaluate to determine performance?
7. On a scale of 0 (for very poor) to 10 (excellent), how would you, apply these characteristics to rate the success of the current policies or measures against online impersonation?
8. How would you measure the efficiency of an assessment system against impersonation?
9. What aspects of the current system do you consider "inadequate"?
10. How would you measure the efficiency of an assessment system against impersonation?
11. How effective is the authentication system against impersonation?
12. In what way can the system be enhanced to fight impersonation?
13. In what ways would you evaluate the enhancements in the context of impersonation?

14. What issues would you focus on when designing an enhanced authentication system?

A6 Concerns of the faculty stakeholder group

i. What does the system aim to achieve?
ii. How does the system aim to achieve this goal?
iii. Can the authentication and security methods guarantee the security of LMS based examination?
iv. How many factors of authentication will the system use?
v. How accurate is the authentication system?
vi. How easy is it to administer the system?
vii. Will the assessment system not hinder the student's progress through the assessment?
viii. Can questions come from a question bank and in a randomized fashion to avoid collusion?
ix. Can the online assessment allow multiple access without loss in security or speed?
x. Will the continuous authentication systems not intimidate the student? Can the process take place in the background but with the student's knowledge?
xi. Will the authentication methods not interrupt the assessment?
xii. Can strict timing apply to the assessment if students take them at different times and from different places?
xiii. How can students familiarize with the authentication scheme ahead of assessments?
xiv. How fair on a student under assessment is the system, given exam pressure?
xv. Can the system ensure that students are allowed the same duration for the assessment?
xvi. The authentication system must have a low error rate i.e. accurate.
xvii. Authentication must not invade student's privacy.
xviii. The system must not be unnecessarily complex to administer.
xix. Can educators have a "live-feed" tool to view students' status and activity during assessment, or authenticate students through continuous random authentication using students' information stored during the course in the databases that guarantee their identity and authentication during the assessment process?
xx. Will students be able to abort the assessment for example, give up or surrender and claim system failure? How can the system discourage or trap such cases?
xxi. Does the system permit the use of diverse assessment activities and assessment strategies?

The main concerns of the educator group relate to the assurance that the right student takes the assessment; the assessment is secure and accurately administered.

Educators generally take an interest in "viewing or seeing" the assessment taking place – so that their interventions (if needed) are timeous and disruptions cause little impact on the overall assessment event. The target was to obtain answers to all SQ1 to SQ4.

A7 Interview questions for the Quality Management Group

1. What is your experience with online assessments?
2. In what ways are you involved in online assessment systems?
3. What conditions would you expect an online assessment to satisfy in order for it to be considered "ideal" from an academic quality perspective?
4. What characteristics of an assessment system do you evaluate to determine performance?
5. What characteristics of an assessment system do you evaluate to determine performance?
6. On a scale of 0 (for very poor) to 10 (excellent), how would you, apply these characteristics to rate the success of the current policies or measures against online impersonation?
7. How would you measure the efficiency of an assessment system against impersonation?
8. What aspects of the current system do you consider "inadequate"?
9. In what ways do you think that impersonation can happen in such an online assessment?
10. How does the online assessment system establish student identity?
11. How would you measure the efficiency of an assessment system against impersonation?
12. How effective is the authentication system against impersonation?
13. What system enhancements would you suggest, to fight impersonation?
14. In what ways would you evaluate the enhancements in the context of impersonation?

A8 Concerns of the Quality Management Group

i. What does the system aim to achieve?
ii. How will the system achieve this?
iii. How many factors of authentication will the system use?
iv. Can the assessment system be available only to students – fully identified and registered for the assessment?
v. All assessments must be quality checked. Will the system allow faculty to quality check questions after uploading to the LMS?
vi. Can assessment questions be derived (during the assessment) from a question bank and randomized to avoid collusion?

vii. Can assessments be timed to happen within a set period?

viii. Does the authentication not invade the student’s privacy?

ix. Can security, as much as possible, be “invisible” to the user to reduce disturbances? The authentication methods used must not interrupt the assessment.

x. How do we measure the authentication mechanism for accuracy? The authentication system must have a low error rate i.e. accurate

xi. How does the assessment system guard against unfair advantage to less financially privileged students?

xii. Does the system provide a “live-feed” tool to view students’ status and activity during assessment? Authentication must not invade the student’s privacy.

xiii. Can the system permit interventions from faculty or management in the event that anomalies happen during the student’s assessment experience?

xiv. Does online assessment allow multiple access without loss in security or speed?

xv. Does the online assessment system comply with the pedagogic values of assessment?

xvi. Does the system permit assessment in various formats and forms such as audio and video, slideshows, animation and simulation?

xvii. Does the system permit the use of diverse assessment activities and assessment strategies?

xviii. Is the assessment system adequately robust to serve the diverse needs of thousands of students, faculty and simultaneously?

The main concerns of this stakeholder group’s concerns are generally quality related and
relate to the assurance that the right student takes the assessment; the assessments are fair for all students in the same cohort, the assessment is secure and accurately administered. Quality Management generally take an interest in ensuring a “good assessment experience” for the student i.e. the need to ensure a low error rate in the system specifically. The system must not influence student assessment experience, but it should facilitate it to the student’s satisfaction. Quality Management are also concerned about the security of the assessment materials (the assessment system and its contents must be inaccessible to unauthorized parties) e.g. that the inputs of each student are correctly identifiable in the system, for safeguarding the reputation of the assessments or the institution. Like the educators’ group, the need for a method of “following up” on students as they take the assessment is necessary. The target was to obtain answers to all SQ1 to SQ4.

A9 Interview questions for the Information Systems Group

1. On what platform is the online assessment system running?
2. What security mechanisms are implemented on the system?
3. How is the system deployed / configured?
4. Does your department provide round the clock monitoring and support services?
5. What is your understanding of “impersonation” in academic assessments?
6. What characteristics of an assessment system do you evaluate to determine performance?
7. On a scale of 0 (for very poor) to 10 (excellent), how would you, apply these characteristics to rate the success of the current policies or measures against online impersonation?
8. How would you measure the efficiency of an assessment system against impersonation?
9. What aspects of the current system do you consider “inadequate”?
10. In what ways can these issues be resolved?

A10 Concerns of the Information Systems Group

i. Latency: In the online assessment what is the time interval between the arrival of a request and the response of the component?

ii. Throughput: What is the volume or number of transactions that the system can do in a second?

iii. Security: How will the institution’s information assets be protected from invasion and cybercrime?

iv. Processing: What is the guarantee that each transaction completes processing?

v. Availability: Is the architecture browser independent?

vi. Future development: Does the architecture provide for scalability and change?

vii. How will the system identify and incorporate data that gets lost because the component was too busy?

viii. Interface: Are the interface and transfer processes between the system that authenticates users and the actual assessment system secure and able to provide timely delivery of the assessment via the interface?

ix. What is the hardware, software and maintenance overhead associated with the system?

x. Is the authentication system open and able to interchange data with standard / popular online assessment systems?

The information systems group’s concerns safeguard the online assessment system and aims to ensure that only authorized users can access the assessment.

The systems developers play a key role in determining the technical feasibility of an architecture by evaluating the architecture from the standpoint of data structures, algorithms, databases and programming tools, methodologies and paradigms.

A11 Interview questions for the Policy Level Stakeholder Group

1. Describe your role in the institution.
2. What are the major responsibilities aligned to your role and position?
3. What are the major goals of your position?
4. To what extent do you influence policy within the organization regarding online assessments?
5. What conditions would you expect an online assessment to satisfy in order for it to be considered "ideal" from your perspective?
6. In summary, what is your understanding of "impersonation"?
7. What characteristics of an assessment system do you evaluate to determine performance?
8. On a scale of 0 (for very poor) to 10 (excellent), how would you, apply these characteristics to rate the success of the current policies or measures against online impersonation?
9. How would you measure the efficiency of an assessment system against impersonation?
10. What aspects of the current system do you consider "inadequate"?
11. What do you consider as major impacts of impersonation in the online assessment environment?
12. What policies or measures are the institution / your role employing in the fight against impersonation in online assessments?
13. How often and by what means are you informed about academic offences in the institution?
14. How often and by what means would you prefer to be informed about academic offences in the institution?
15. How would you measure the efficiency of an assessment system against impersonation?
16. On a scale of 0 (for very poor) to 10 (excellent), how would you rate the success of the current policies or measures against online impersonation?
17. Would you please elaborate on your rating?
18. Where does the current system fall short of your expectation in fighting against impersonation?
19. What features, characteristics would you expect or recommend be included in an online assessment system, focusing mostly on fighting impersonation?
20. What general characteristics would you take into account when evaluating a method or tool that fights impersonation?
21. What kind of assessment experience do you want to create in your institution?

22. In your view, what would make a redesign of the online assessment system successful?

A12 Concerns of the policy group

i. How the system impacts on the quality of assessment and qualifications?
ii. The cost implications of the proposal.
iii. The impact of the proposed architecture on operations related to assessment.
iv. The implications on student, staff and other stakeholders' interactions.
v. The permanency of the solution.
vi. The impact on student pass rates.
vii. The alignment of the assessment (and qualifications) to the regulation imposed by industry.
viii. What competitor institutions offer for the same issues and challenges.

The Policy Makers desire that assessments be conducted in a manner that meets the expectations and requirements of the institution and higher authority such as the Department of Education and Industry at large. The assessments must be of credible.

APPENDIX B: STAKEHOLDER SCENARIOS

B1 Student interaction with the online assessment system

Using the data collected from the student and parent stakeholder groups, the following design models for the online assessment system evolved.

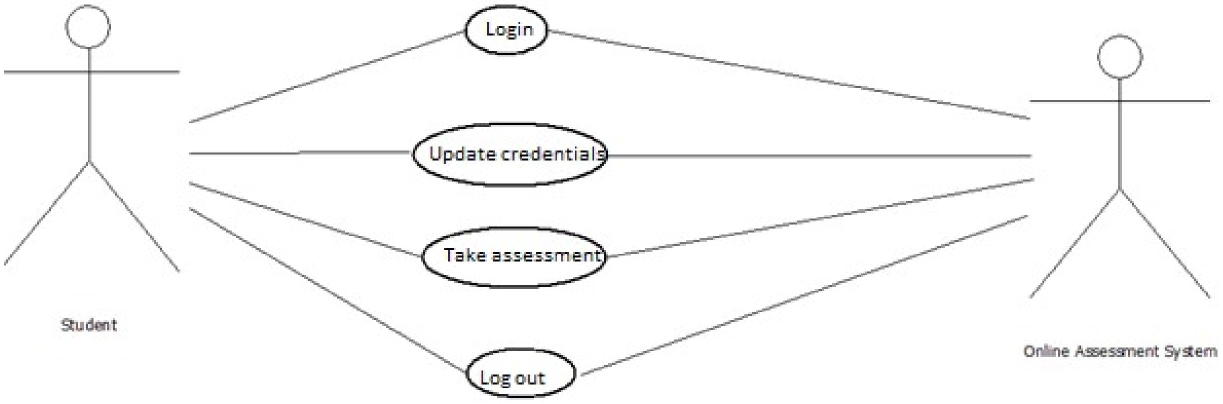


Figure B1: Student interaction use – case diagram

B2 Faculty / Educator interaction with the online assessment system

The educator group interacts with the online assessment system in various ways such as creating content and overseeing assessments as they take place. Educators also require the capacity to intervene with assessments for example, when students face technical difficulty or fraud is suspected.

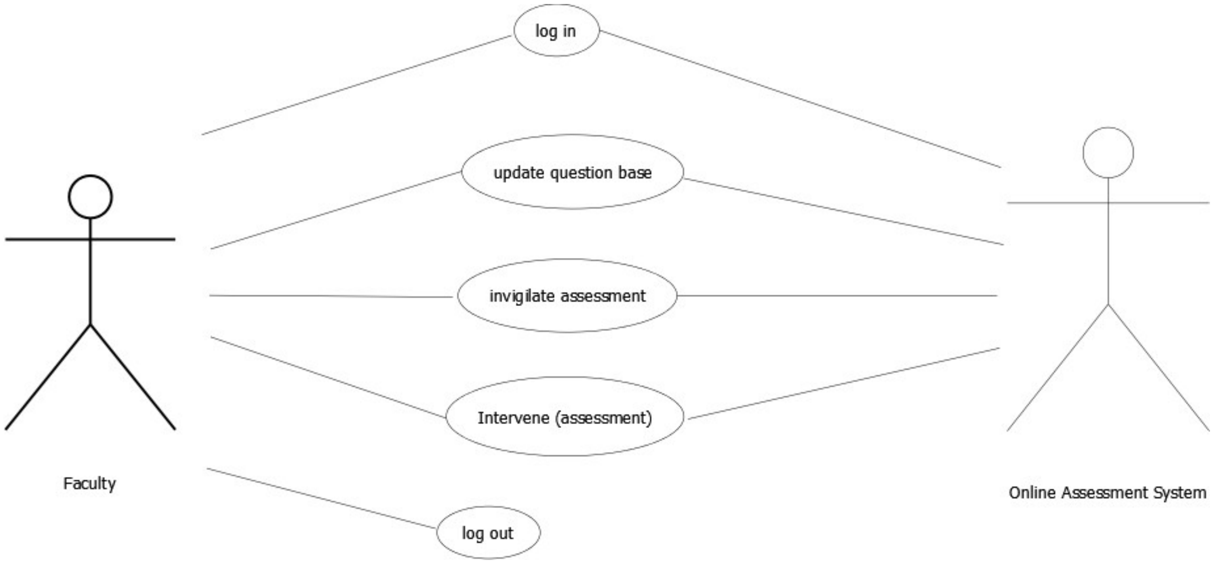


Figure B2: Faculty use case diagram

B3 Quality managers' interaction with the online assessment system

The quality management group interacts with the online assessment system in various ways such as editing, validating assessment content, overseeing the work of faculty, and monitoring system performance during assessments. Quality managers have the capacity to intervene with assessments such as when students face technical difficulty or fraud is suspected.

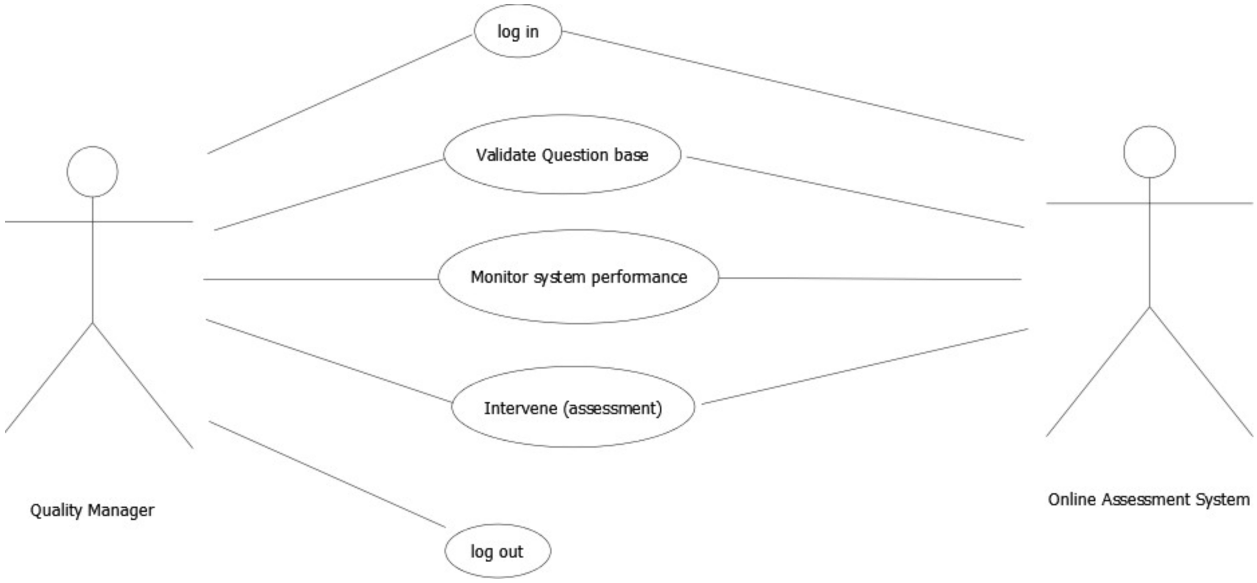


Figure B3: Quality group use case diagram

B4 Information Systems group's interaction with the online assessment system

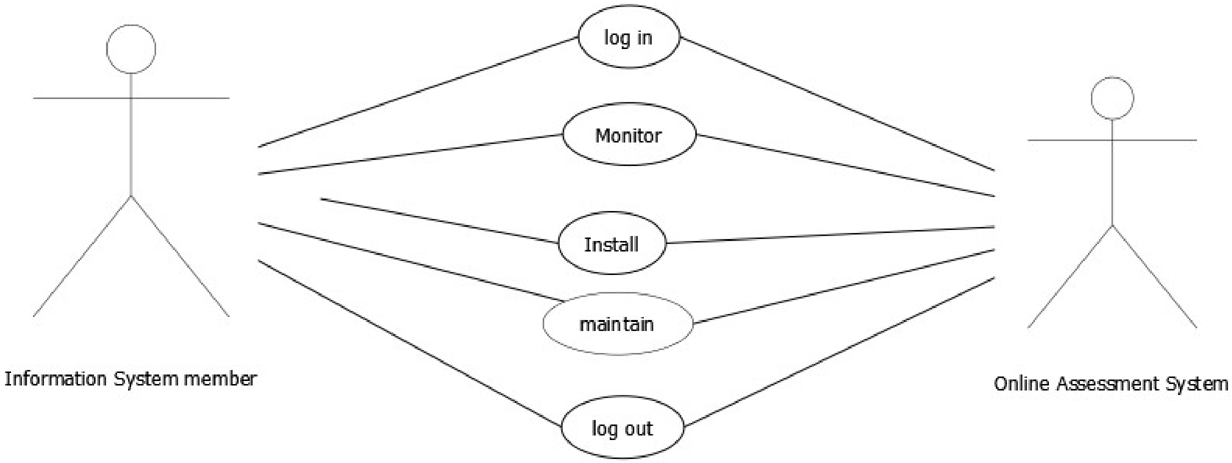


Figure B4: Information Systems group use case

B5 Policy making group’s interaction with the online assessment system

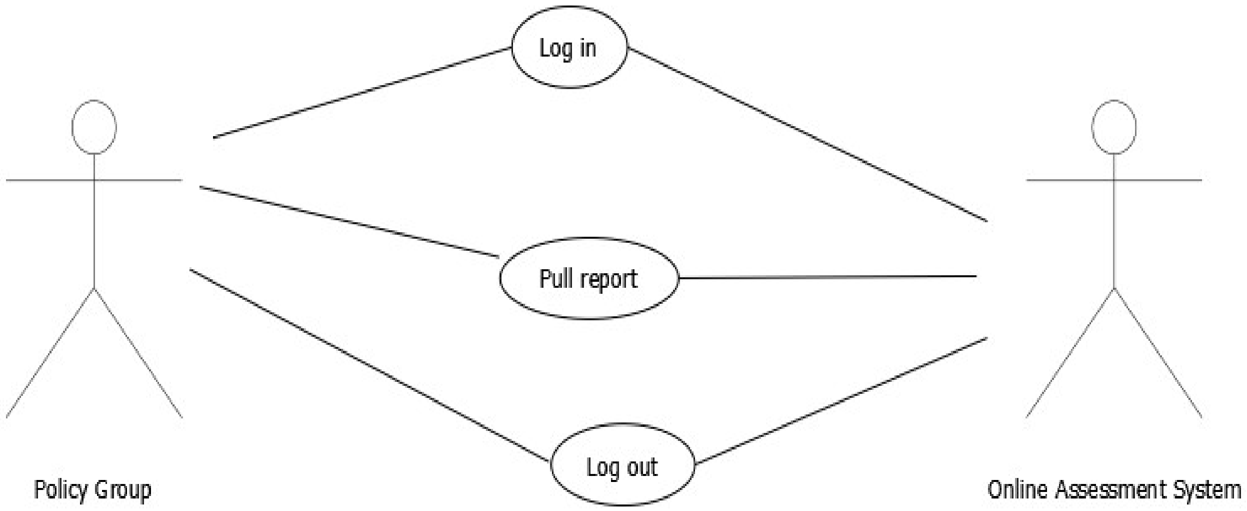


Figure B5: Policy group use case

APPENDIX C: A CANDIDATE ARCHITECTURE FOR A SECURE ONLINE ASSESSMENT SYSTEM

C1 Overview

After collecting stakeholder concerns and applying the principles of architectural design, a candidate software architecture for the design of online assessments that fights impersonation was derived. The discipline of software architecture design uses views as vehicles that software architects use to focus on certain aspects of the system architecture. The IEEE 1471(2000) qualifies the architecture views as a function of the concerns of stakeholders and provide a way to communicate an architecture with stakeholders.

C.2 Description of the proposed architecture

The description of the proposed software architecture is broken down into 4 + 1 views (Lange et al., 2006) namely:

A. The logical view
B. The process view
C. The deployment view
D. The physical view

These different views are explained in the following sub-sections.

C2a Logical view

In the online assessment system, users perform different operations as detailed in the functional requirements of the Learning Management System. The Identity Management System (IMS) is responsible for authenticating users, at the start and during the online assessment through multifactor authenticators.

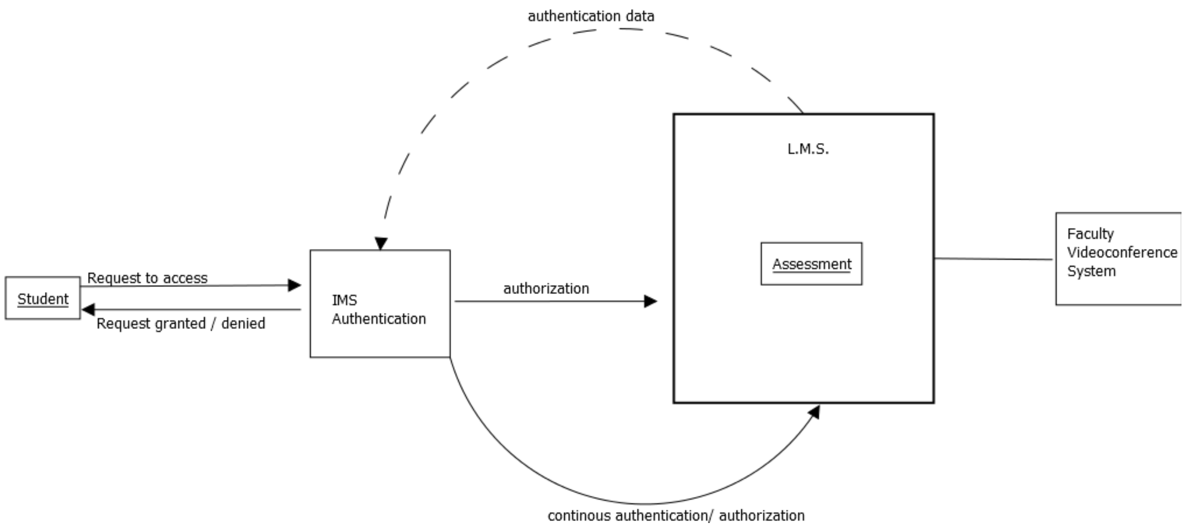
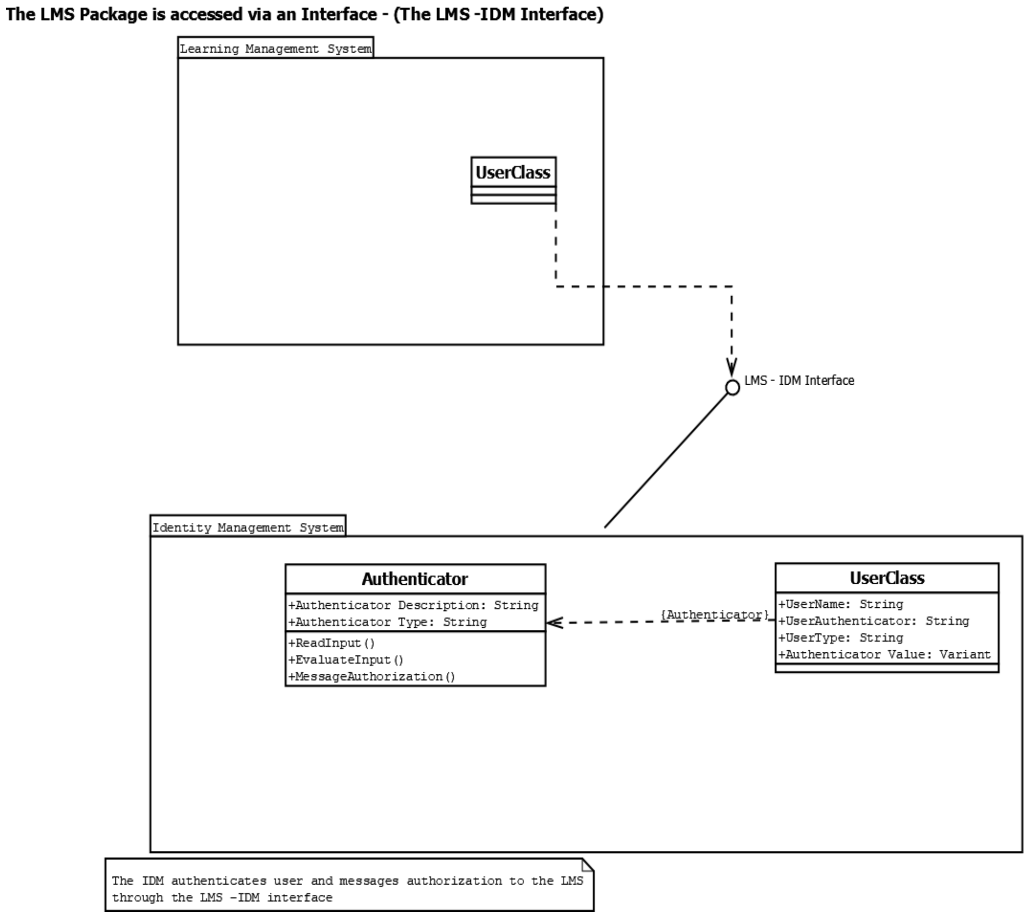


Figure C1: Proposed online assessment system

The Learning Management System (LMS) and the Identity Management System (IMS) communicate with each other via an interface that facilitates two-way exchange of authentication data and authorizations. Figure C2 summarizes the structure of the LMS package relationship.


The LMS Package is accessed via an Interface - (The LMS -IDM Interface)
Learning Management System
UserClass
LMS - IDM Interface
Identity Management System
Authenticator
+Authenticator Description: String
+Authenticator Type: String
+ReadInput()
+EvaluateInput()
+MessageAuthorization()
{Authenticator}
UserClass
+UserName: String
+UserAuthenticator: String
+UserType: String
+Authenticator Value: Variant

The IDM authenticates user and messages authorization to the LMS through the LMS -IDM interface

Figure C2: IMS – LMS interface

The system combines authenticators from all three specializations (knowledge-based, possession-based and biometric) to generate authentication data that is used to authorize an assessment to commence and proceed (Figure C2a).

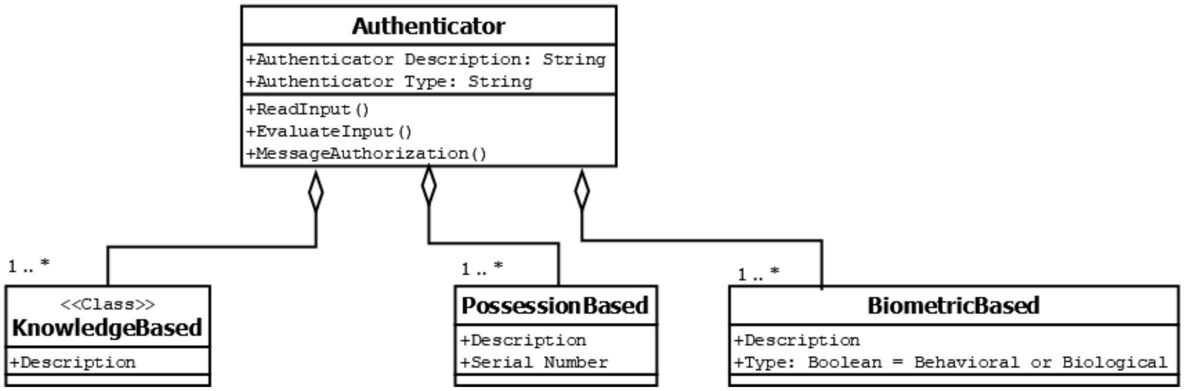


Figure C2a: Types of authenticators

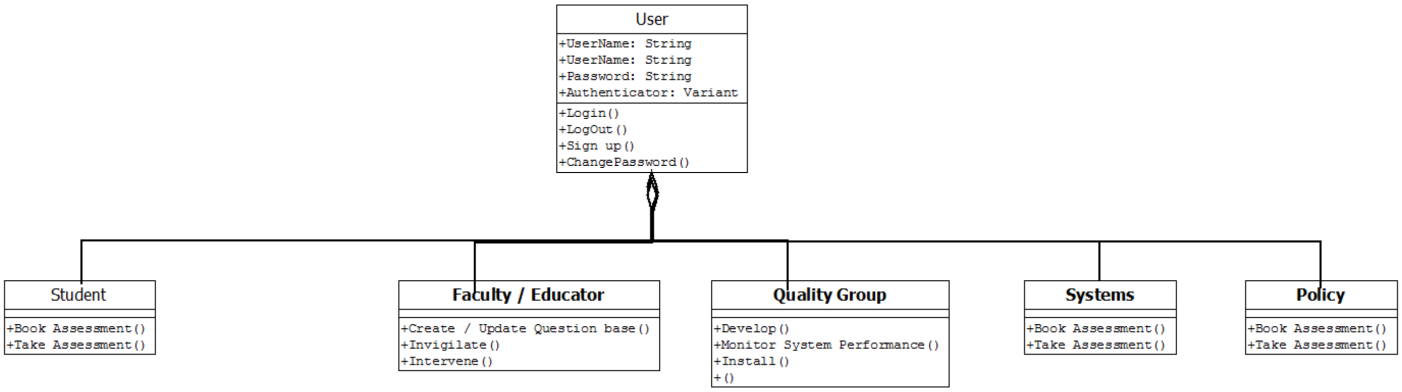
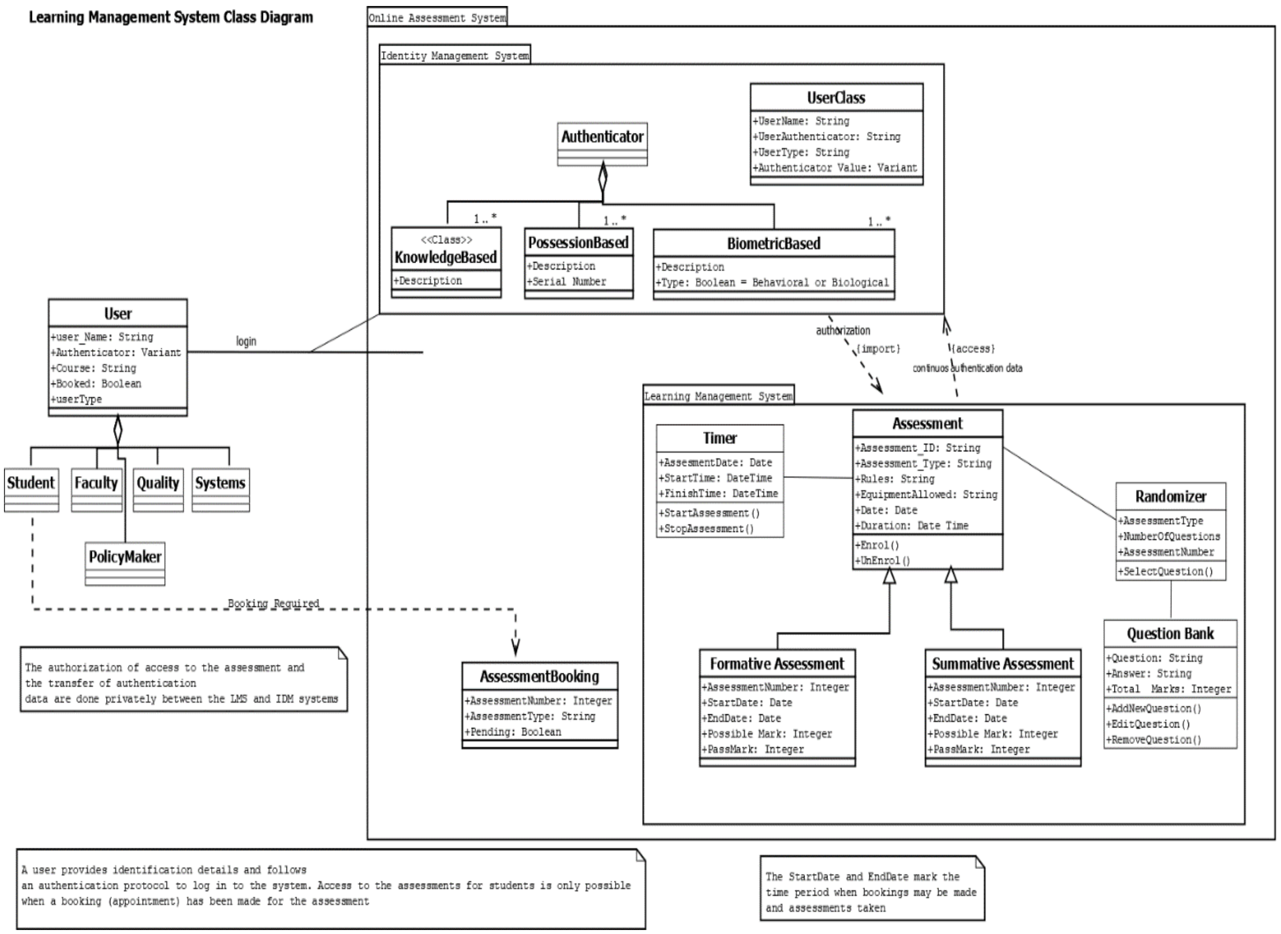


Figure C2b: Stakeholder groups

The user Class shown in Figure C2 generalizes users as student, faculty, / educator, quality group, systems and policy in line with the stakeholder classification outlined in Section 3.7.2. This is elaborated in Figure C2b as a UML class aggregation/specialization diagram.

The LMS defines the exact rights and privileges of the individual users. Figure C3 is a class diagram that shows the entities that interact in the system when a student attempts an assessment. The diagram shows two types of assessments that the student may engage in - formative assessments during the course of study and summative assessments towards completion.



The authorization of access to the assessment and
the transfer of authentication
data are done privately between the LMS and IDM systems

A user provides identification details and follows
an authentication protocol to log in to the system. Access to the assessments for students is only possible
when a booking (appointment) has been made for the assessment

The StartDate and EndDate mark the
time period when bookings may be made
and assessments taken

Figure C3: Proposed system class diagram

When a student feels ready to take an online assessment, they are required to make a booking. The LMS records the booking for use as a condition for accessing the assessment. The booking details are stored on the system and availed to other stakeholders like faculty staff for the purposes of monitoring, and the systems group for system performance monitoring.

Figure C4 shows that in order to access an assessment the student needs to log onto the system using a unique username and password combination (Knowledge-Based-Authenticator). If and only if both, the username and password match the entries on the student database, can the user access to continue. When these matches an entry on the student's database, the IMS generates a One-Time-Personal Identification Number (OTP).

The IMS then uses the Short Message Service to send the One-Time-PIN to the student's registered mobile phone (Possession-based Authentication).

On receipt of the SMS, the student must capture the OTP into the system so that the IMS can authenticate the username and password, and the system-generated OTP. The IMS locator component then identifies the geographical location of the sending cellular phone.

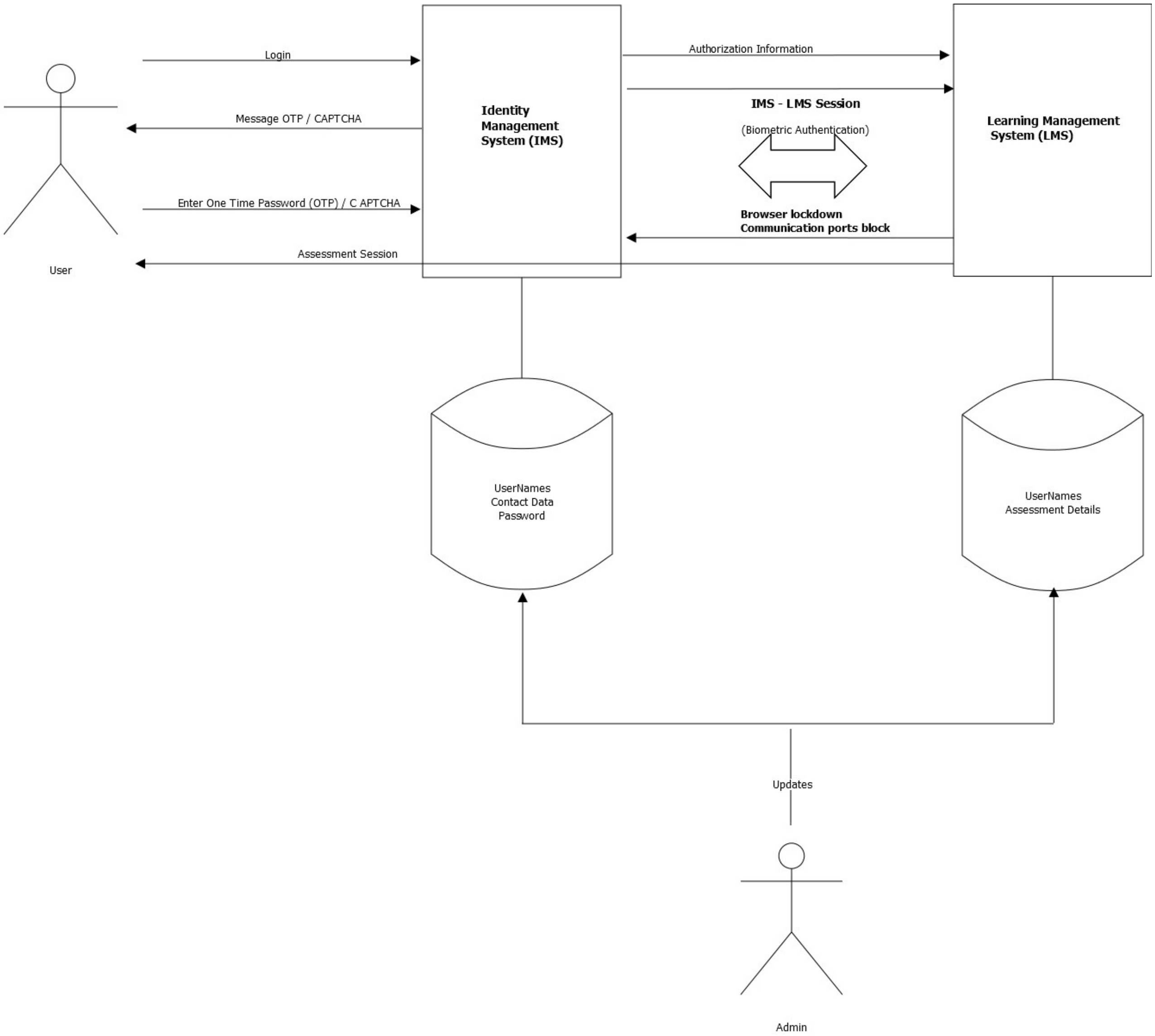

Login
Message OTP / CAPTCHA
Enter One Time Password (OTP) / C APTCHA
Assessment Session
User
Identity Management System (IMS)
Authorization Information
IMS - LMS Session
(Biometric Authentication)
Browser lockdown
Communication ports block
Learning Management System (LMS)
UserNames
Contact Data
Password
UserNames
Assessment Details
Updates
Admin

Figure C4: Log on procedure

When the username, password, and the system generated OTP perfectly match, the IMS then "locks" the student's computer to quarantine the student from external interference and participation.

This lock process is achieved as follows:

1. The student's browser and other communication ports are "locked down" i.e. blocked. This means that the student cannot open new windows or tabs in the browser, but only the online assessment remains active on the student's computer system.
2. Communication ports on the student's computer are blocked. Ports that can be used for printing, instant messaging, multiple screens display or screen sharing using software such as TeamViewer™ or Any Desk™ become unusable and the student's computer quarantined with only one display unit viewing the assessment.
3. The Internet Protocol (IP) address of the student's computer is traced and from it the student's assessment session is mapped to Machine Access Control (MAC) address of the student's computer.
4. The geographical location of the student's computer is determined. To proceed, this must match the location of the cellular device that returned the OTP.
5. The camera and microphone on the student's computer are remotely switched on.
6. The student shows the Identity Card issued by the Institution by holding it up for a few moments while facing the camera.
7. Facial recognition and authentication take place using the ID card and anatomical features of the student. A match in both cases is necessary to proceed to the assessment.
8. Non-academic fraud / code of honour is displayed on the student screen. The content is read out loud to the student.
9. Student verbally subscribes to an anti-fraud statement.
10. The student may be asked to answer some challenge questions derived from their record on the database (Ullah et al., 2014).
11. The student is logged onto the assessment – when all authentication is cleared.
12. The assessment timer starts, and the student assessment begins.
13. As the assessment proceeds, biometric data such as mouse dynamics, video / camera images and video and keystrokes are captured and transmitted to the IMS. Each packet of data is "signed" with the MAC address of the device that captures it. For example, each image or video captured is captioned with a timestamp and MAC signature.

Figure C5a elaborates steps 1 to 12 in an activity diagram. Step 13 is elaborated in Figure C5b.

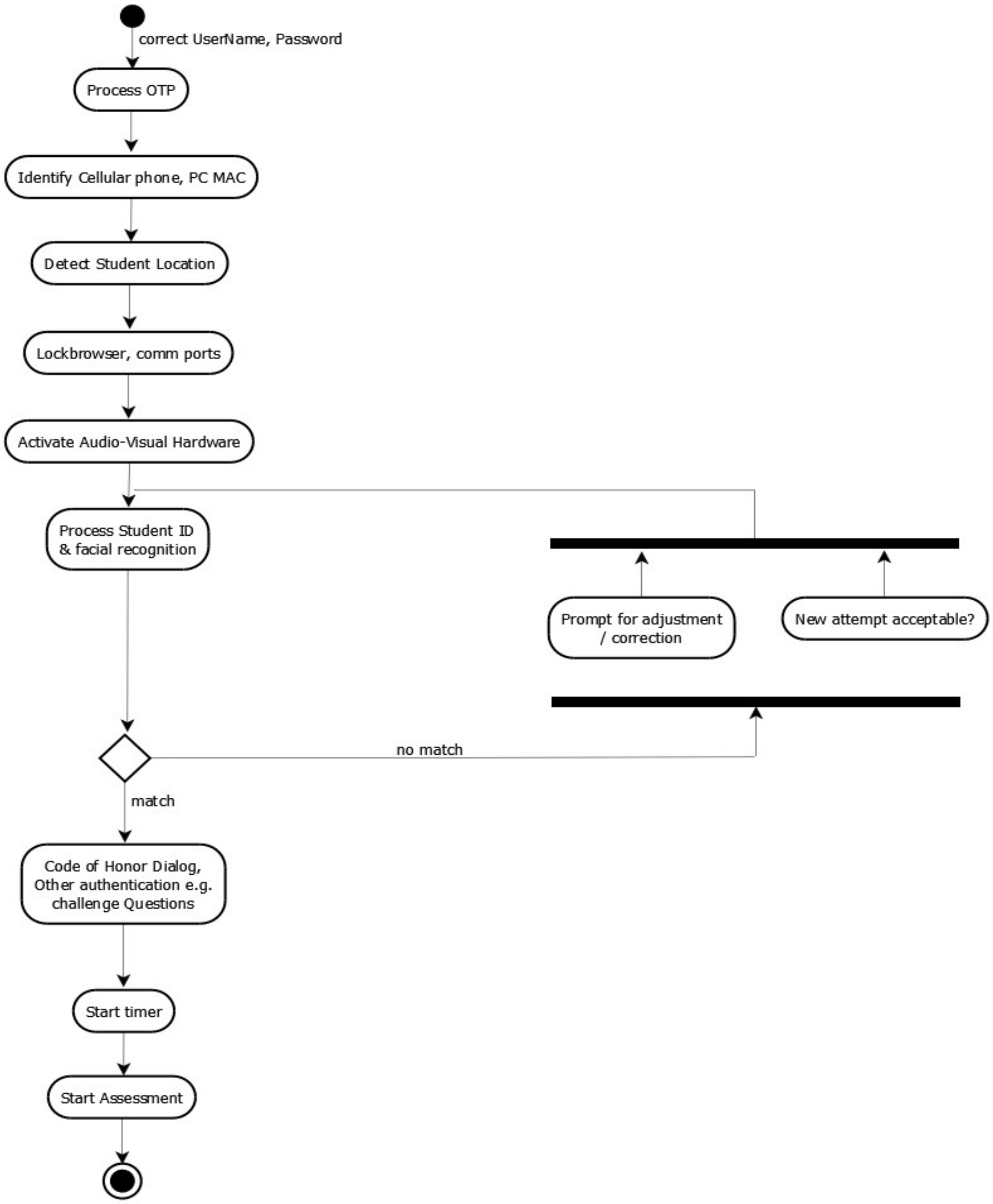

correct UserName, Password
Process OTP
Identify Cellular phone, PC MAC
Detect Student Location
Lockbrowser, comm ports
Activate Audio-Visual Hardware
Process Student ID & facial recognition
Prompt for adjustment / correction
New attempt acceptable?
no match
match
Code of Honor Dialog, Other authentication e.g. challenge Questions
Start timer
Start Assessment

Figure C5a: Student log on activity diagram

As the assessment proceeds, biometric authentication data such as mouse, keyboard dynamics, or camera-generated video, still photographic images and predicative authentication information (geographical location of the student's computer) pass across the LMS - IMS interface for continuous authentication in the IMS. In the optimum situation, Artificial Intelligence can be used to monitor head and eye movements during assessment.

Artificial Intelligence (AI) is one technological option that can automate remote invigilation and interventions in the event that possible cases of impersonation arise. This extension in the technology to incorporate AI would ensure that the student focused on the assessment and not communication with a third party and also cut down the costs of the assessment system in the long term.

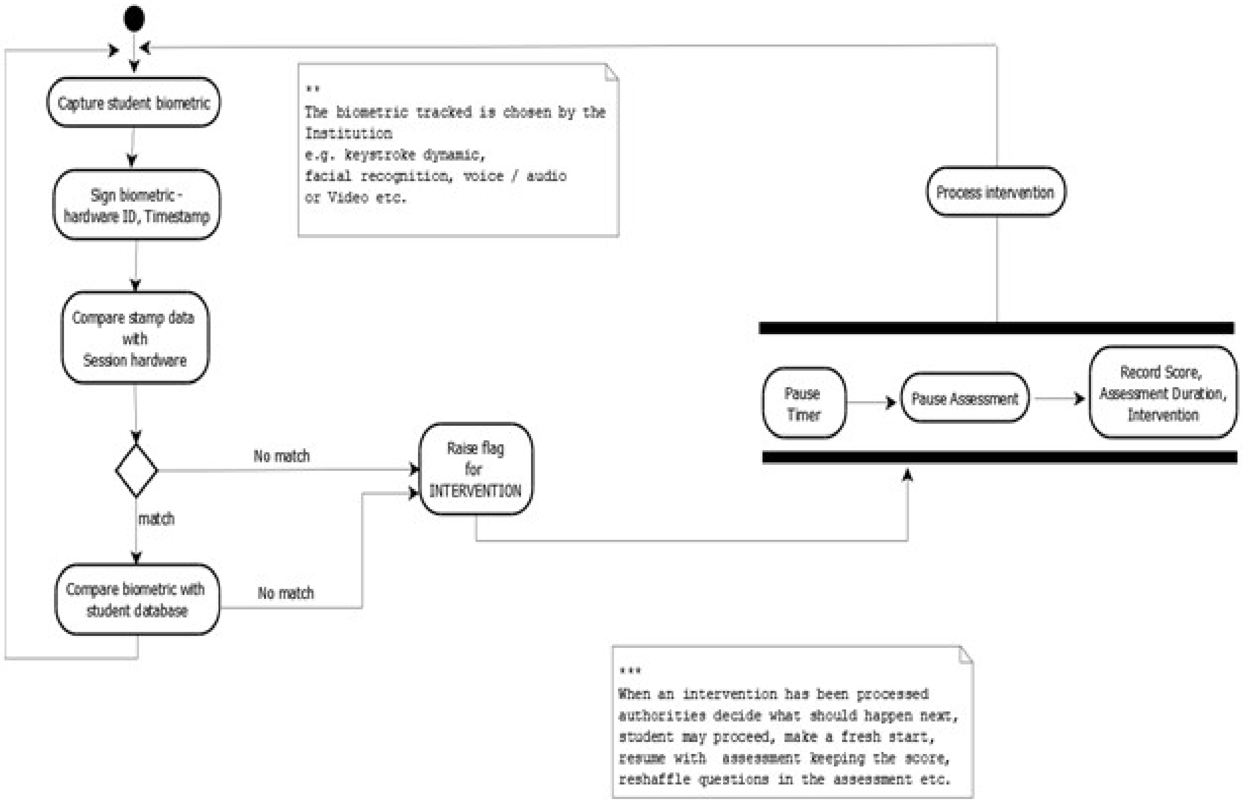

Capture student biometric
Sign biometric - hardware ID, Timestamp
Compare stamp data with Session hardware
No match
match
Raise flag for INTERVENTION
Compare biometric with student database
No match
**
The biometric tracked is chosen by the Institution
e.g. keystroke dynamic,
facial recognition, voice / audio
or Video etc.
Process intervention
Pause Timer
Pause Assessment
Record Score, Assessment Duration, Intervention
***
When an intervention has been processed
authorities decide what should happen next,
student may proceed, make a fresh start,
resume with assessment keeping the score,
reshaffle questions in the assessment etc.

Figure C5b: Example activity diagram for proposed architecture

For each authenticator, the system analyses the captured reading against the contents of the students' database and assessment record. Only a match on all authenticators provides or continues to provide access to the assessment (Figure C6).

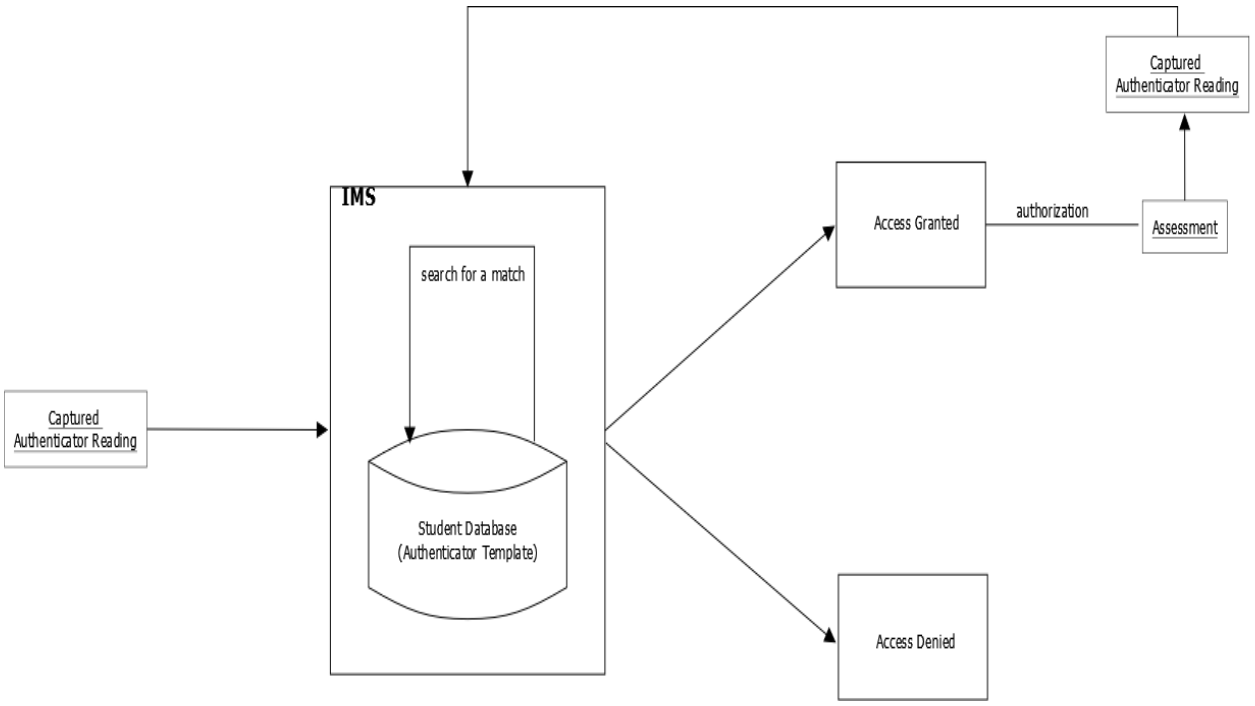

Captured Authenticator Reading
IMS
search for a match
Student Database (Authenticator Template)
Access Granted
authorization
Assessment
Captured Authenticator Reading
Access Denied

Figure C6: Processing authentication data

C2b Process view

The following interaction diagrams show the important runtime interactions between the parts in the context of collaboration to reach a common goal. Figure C7 shows the state machine diagram clarifying how the system processes the student's authentication at the beginning of the assessment and during the assessment.

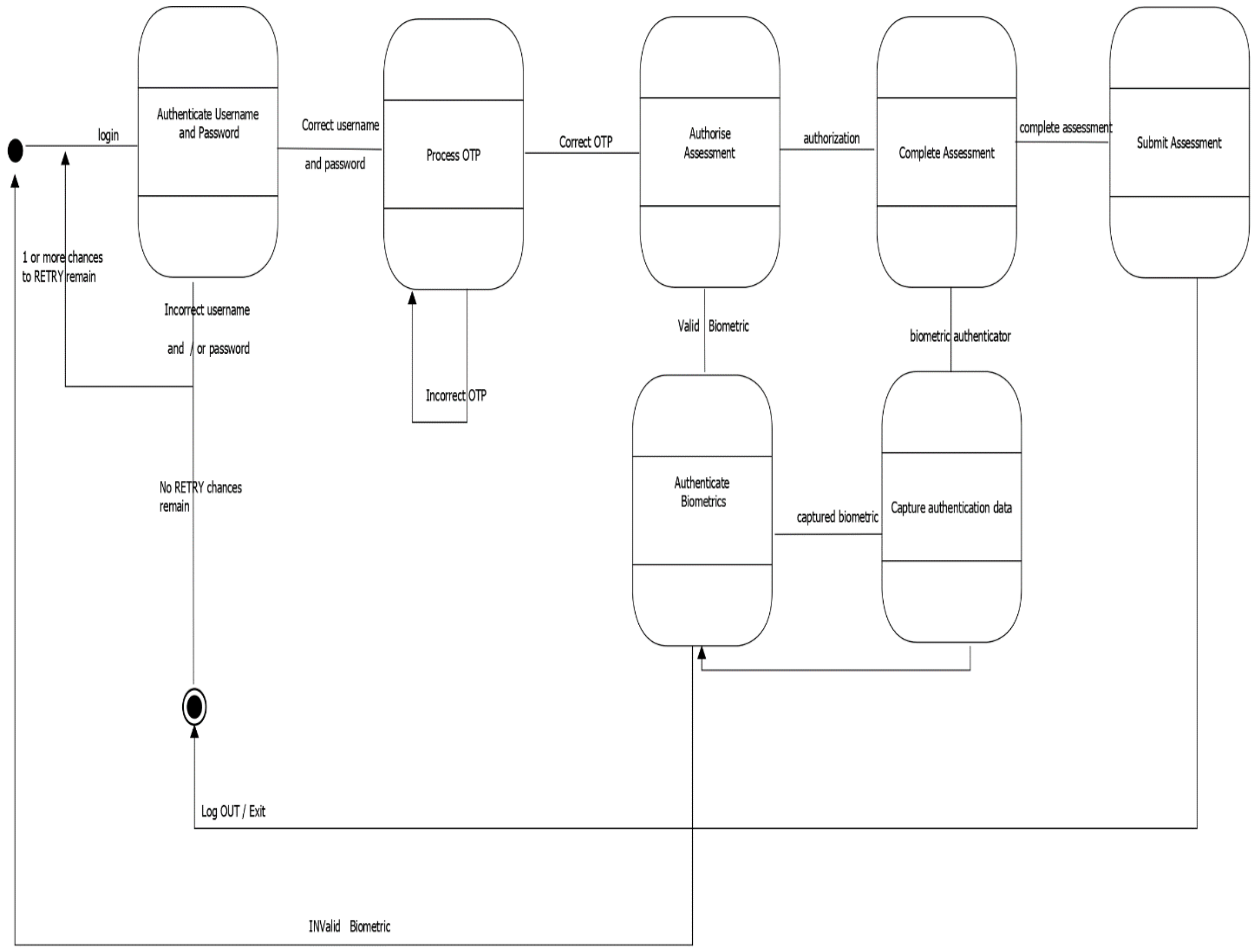


Figure C7: State machine diagram

The process of student authentication is clarified further in Figures C8. Figure C9 is an activity diagram specific to the student logging in to take the online assessment. Figure C9 illustrates the process view of the system in the form of a sequence diagram.

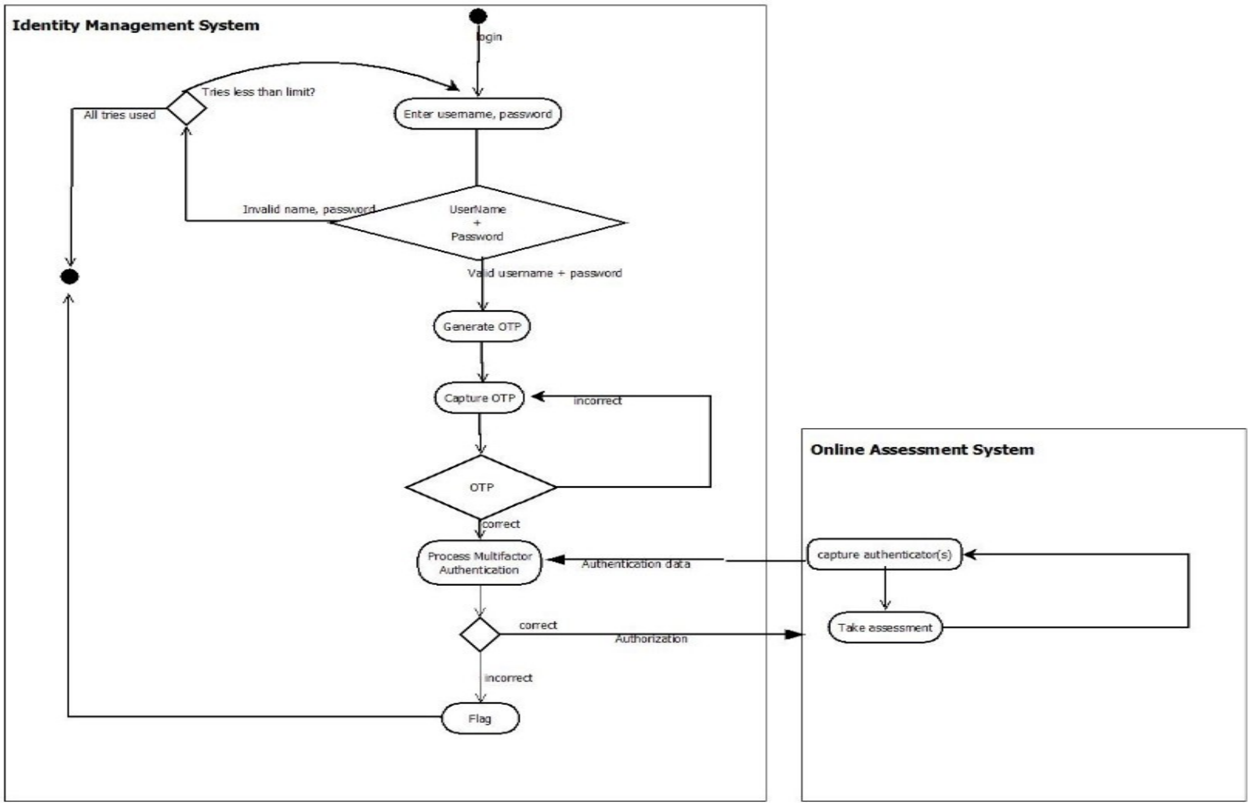


Figure C8: Activity diagram

The sequence diagram shown in Figures C9a to Figure C9c visually shows the high level order of interaction and the messages that are exchanged between the student and the assessment system during logon components and the timing of events.

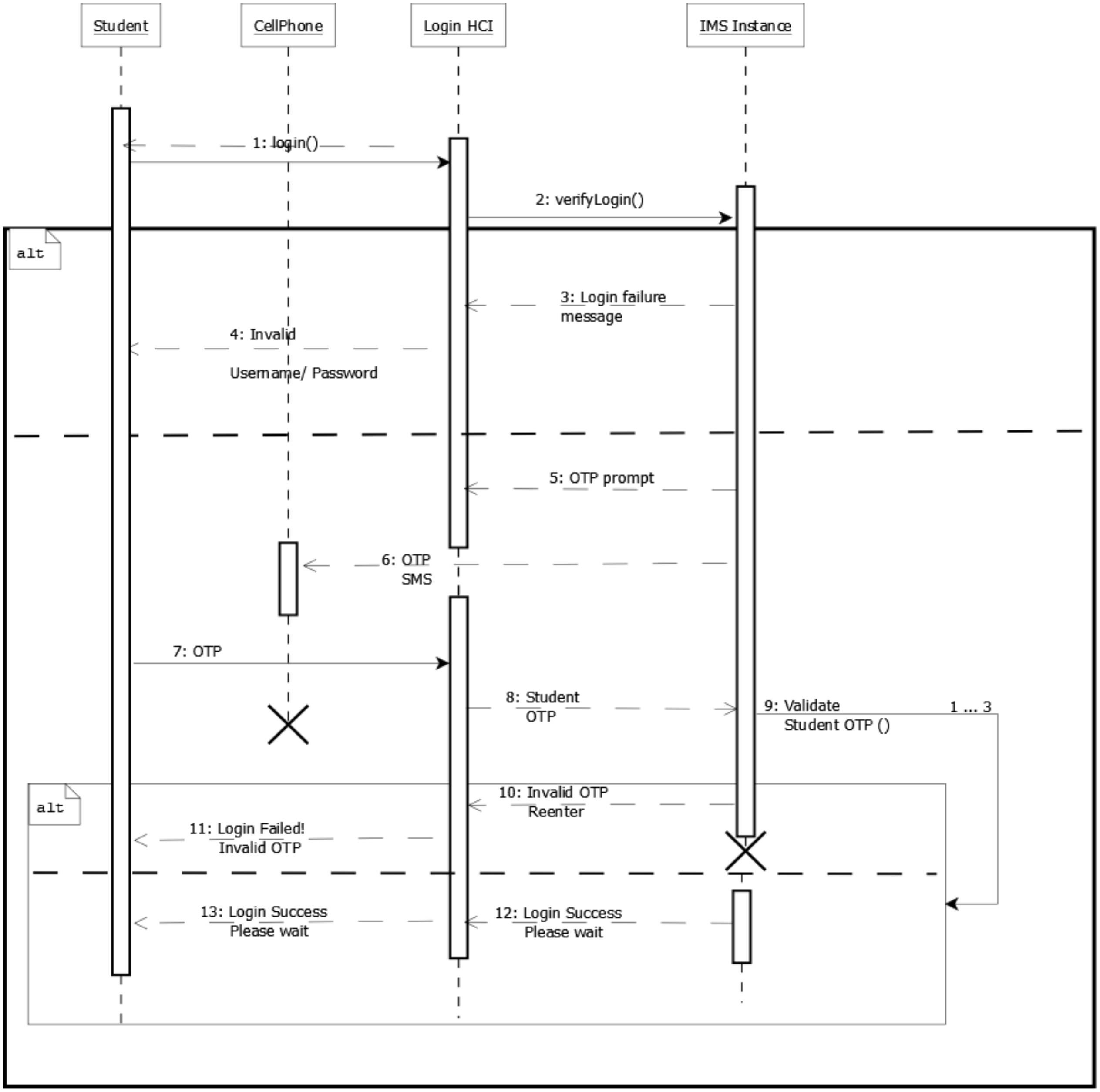


Figure C9a: Sequence diagram

On successful log on to the IMS, the student's computer is accessed, and a secure assessment environment is established by identifying and locking down the student's computer; restricting connectivity to the assessment only.

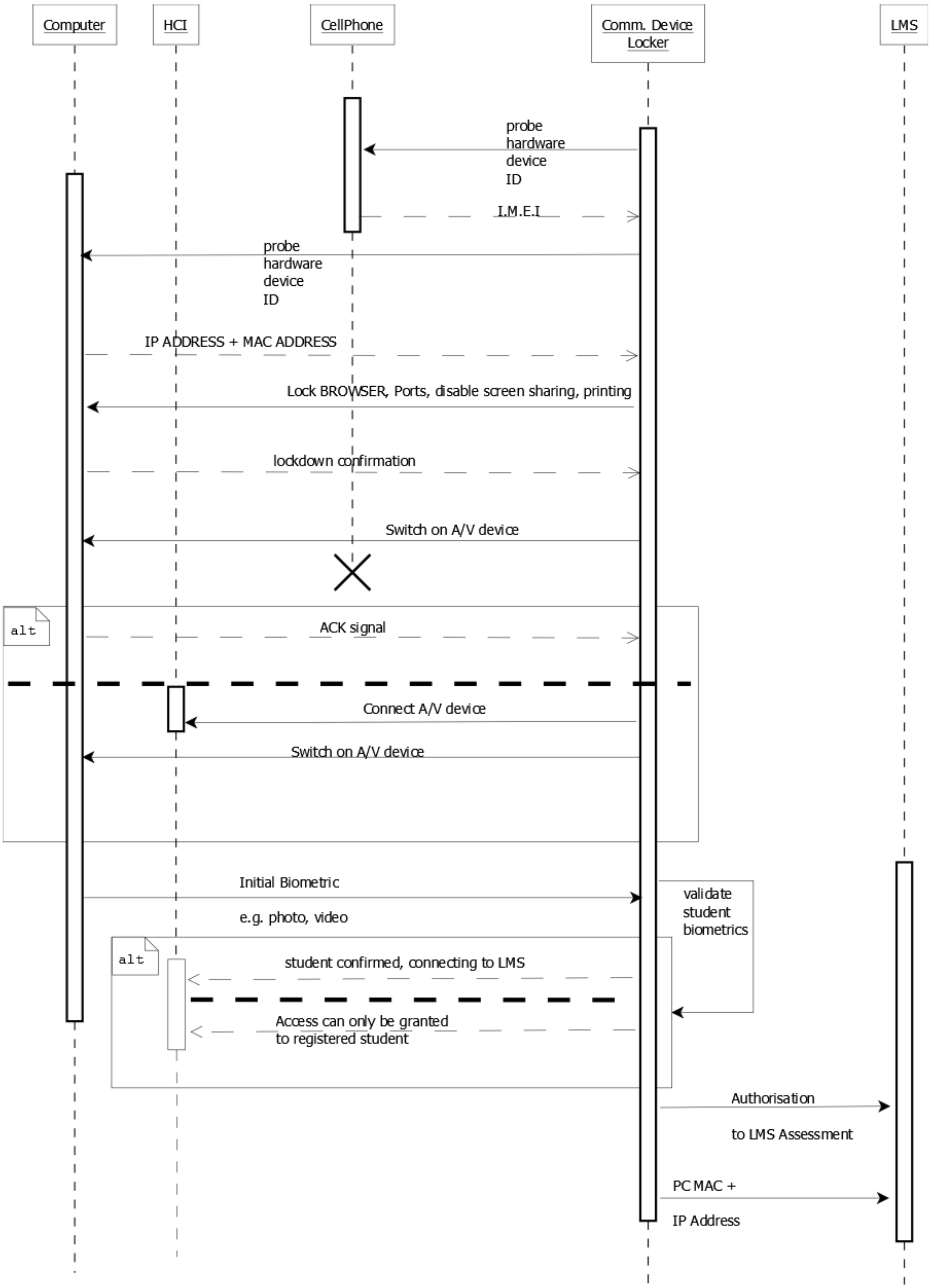


Figure C9b: Lockdown of student device

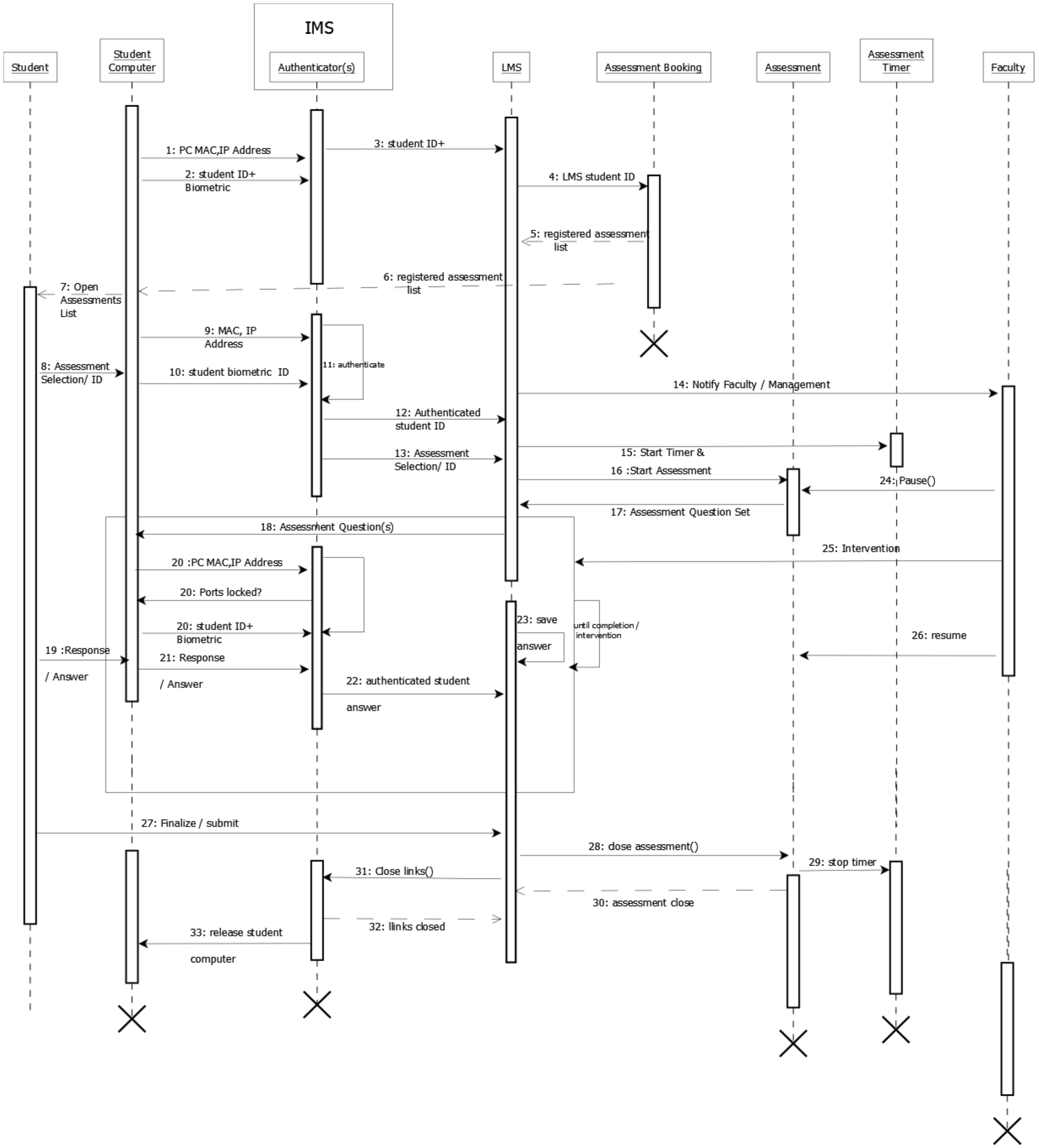


Figure C9c: Engagement in assessment

C2c Deployment view

The system is comprised of modules that follow the “pipe and filter” protocol to interchange data and control signals. Data is processed within the components and messages or intermittent results of processing are relayed between components through pipes.

All activities take place across secure internet connection. The component diagram (Figure C10) shows the component diagram for the proposed system that authenticates users in an online assessment system.

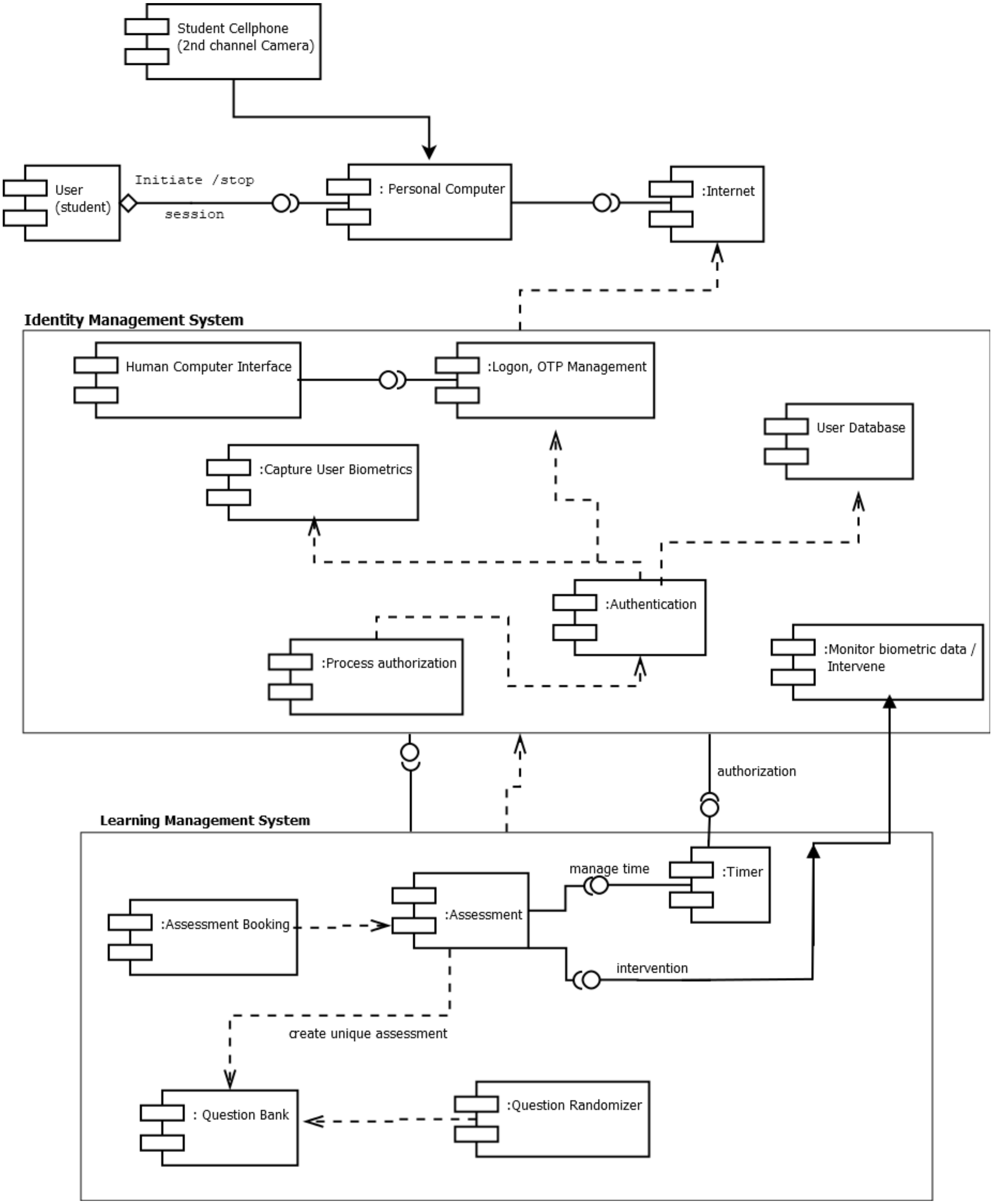


Figure C10: Component diagram

C2d Physical view

This view shows how the components of the online assessment system exist in the real world. Figure C11 and Figure C12 show how the components of the system interlink in the online assessment system.

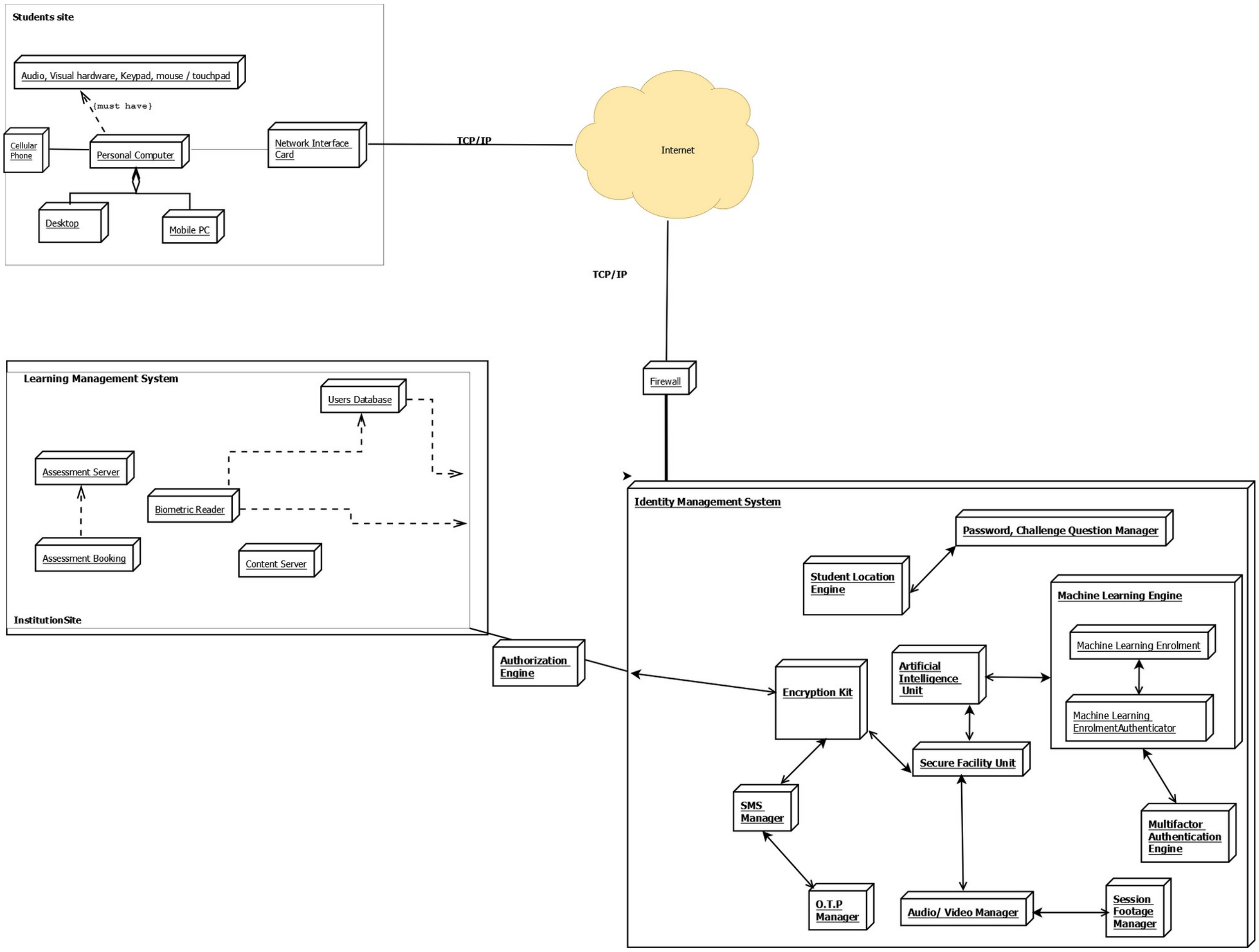


Figure C11: Deployment diagram

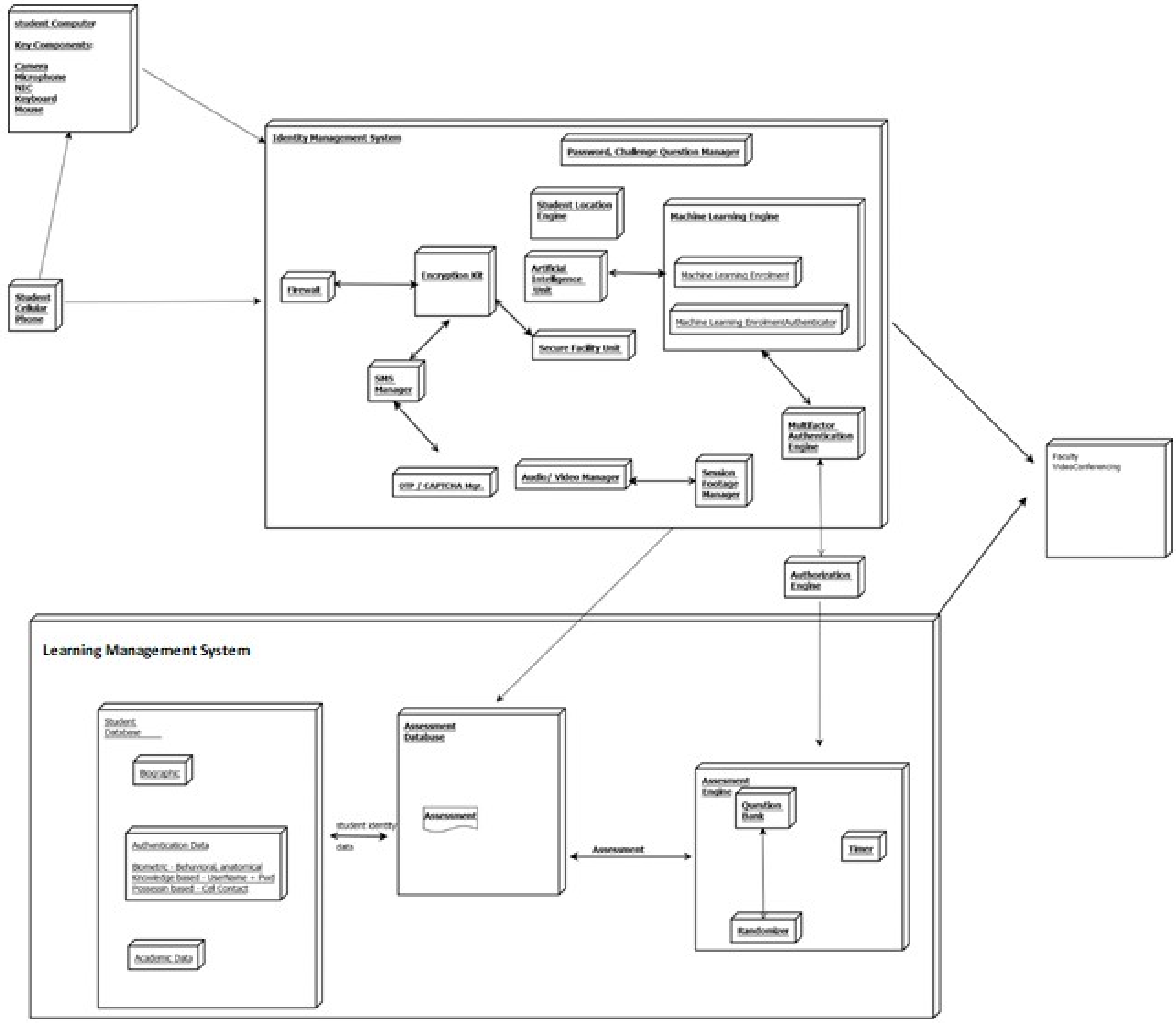


Figure C12: Deployment diagram 2

C2E Scenarios

The 4 + 1 defines scenarios as a distinct view. Each scenario represents the different set of processes, actions and interactions that can take place within the system. The activity diagrams shown in Figure C5 and Figure C8 and the sequence diagram shown in Figure C9A represent some of the important scenarios associated with the online assessment system.