

2024

## **Student Attitudes and Intentions to Use Continuous Authentication Methods Applied to Mitigate Impersonation Attacks During E-Assessments**

Andrea E. Green

Follow this and additional works at: [https://nsuworks.nova.edu/gscis\\_etd](https://nsuworks.nova.edu/gscis_etd)



Part of the [Databases and Information Systems Commons](#), [Information Security Commons](#), and the [Instructional Media Design Commons](#)

## **Share Feedback About This Item**

---

This Dissertation is brought to you by the College of Computing and Engineering at NSUWorks. It has been accepted for inclusion in CCE Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact [nsuworks@nova.edu](mailto:nsuworks@nova.edu).

Student Attitudes and Intentions to Use Continuous Authentication Methods  
Applied to Mitigate Impersonation Attacks During E-Assessments

by

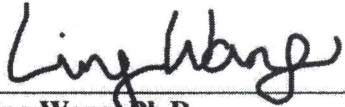
Andrea E. Green

A dissertation submitted in partial fulfillment of the requirements  
for the degree of Doctor of Philosophy  
in  
Information Systems

College of Computing and Engineering  
Nova Southeastern University

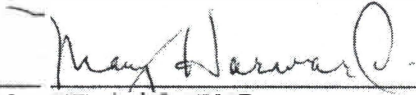
2024

**We hereby certify that this dissertation, submitted by Andrea Green conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.**



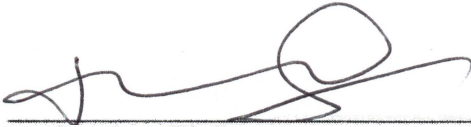
\_\_\_\_\_  
**Ling Wang, Ph.D.**  
**Chairperson of Dissertation Committee**

1/16/24  
**Date**



\_\_\_\_\_  
**Mary Howard, Ph.D.**  
**Dissertation Committee Member**

1/16/24  
**Date**



\_\_\_\_\_  
**Junping Sun, Ph.D.**  
**Dissertation Committee Member**

1/16/24  
**Date**

**Approved:**



\_\_\_\_\_  
**Meline Kevorkian, Ed.D.**  
**Dean, College of Computing and Engineering**

1/16/24  
**Date**

**College of Computing and Engineering**  
**Nova Southeastern University**

**2024**

An Abstract of a Dissertation Submitted to Nova Southeastern University  
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Student Attitudes and Intentions to Use Continuous Authentication Methods Applied to  
Mitigate Impersonation Attacks During E-Assessments

by

Andrea E. Green  
January 2024

No solution can ultimately eliminate cheating in online courses. However, universities reserve funding for authentication systems to minimize the threat of cheating in online courses. Most higher education institutions use a combination of authentication methods to secure systems against impersonation attacks during online examinations. Authentication technologies ensure that an online course is protected from impersonation attacks. However, it is important that authentication methods secure systems against impersonation attacks with minimal disruption during an examination. Authentication methods applied to secure e-assessments against impersonation attacks may impact a student's attitude and intentions to use the e-examination system.

In this regard, the research study investigated student attitudes and intentions to use examination software that requires continuous authentication to protect the system against impersonation attacks. This research examined how student attitudes and intentions to use continuous authentication methods applied to e-assessment security are related to students' performance expectancy, effort expectancy and privacy concerns. In addition, the investigation explored how these constructs are also related to trust and perceived risks associated with using the system.

Utilizing the Unified Theory of Acceptance and Use of Technology Model (UTAUT) conceptual framework, this quantitative study extracted associated constructs from the literature to employ an instrument that measures students' perceptions on continuous authentication methods which are designed to mitigate impersonation attacks during e-exams including proctoring, webcam monitoring and lock-down browsers. Findings suggest that factors such as performance expectancy, effort expectancy and privacy concerns may significantly influence a student's behavioral intentions and attitudes during e-exams. Furthermore, these perceptions also extend to impact students' perceived risks when interacting with the authentication system and may be contingent on levels of trust depending on the technology. The findings underscore the importance of understanding student perspectives in shaping their experiences with authentication technologies.

## Acknowledgements

This dissertation has been one of the most challenging yet fulfilling endeavors of my life. I am grateful for my village, everyone who has supported me throughout this humble educational experience. I have immense gratitude for your generous support.

First, I would like to thank my dissertation committee chair, Dr. Ling Wang. This accomplishment would not have been possible without your support, guidance, and mentorship. Your help and support mean more to me than you would ever know. Your critique of my work was essential to get me through the process. I appreciated every step of your guidance, and I am grateful and honored to have worked with you to accomplish this life goal. I also would like to thank my committee members Dr. Mary Harward and Dr. Junping Sun who were both instrumental in ensuring the progress of this research and who were both essential in getting me through the dissertation process. I appreciate your feedback and all the time you took to review my research and provide me with valuable guidance and advice.

For my mother, Elizabeth, I would like to thank you for expressing your faith in me when it really mattered and your hard work and sacrifice to get me to this point. For my daughter Empress-Tsyah, I hope I have made you proud, just as you have always made me honored to be your mother. Thank you for your love and support and believing in me the way no one else can.

For my husband, Eddy, thank you for your patience, love and understanding. I am grateful for all your support and encouragement. I thank you for always pushing me, and your words of inspiration whenever I became discouraged. To my mother-in-law, Elisabeth, I am grateful for your comforting support. My siblings, Edgar, and Erma, you have given me a noteworthy example to follow and Curtis, Aurelie and Edmund, I have learned so much from all of you, you all inspire me.

I am also grateful for many friends and mentors who helped me to maintain my balance throughout the process. For Linda Lara, thank you for being a true friend. I thank Dr. Nicki Fraser, Dr. Todd Lengnick and Dr. Karen Clay for pushing me to finish.

Finally, I am very grateful for Dr. Julia Parker, thanks for all your guidance and support in helping me to better understand the methods and data analysis portion of this research. You have given your valuable time to shape, nurture, and tutor me and without you, this would not be possible. Finally, to Dr. Dionne Stevens, my friend and mentor, you were one of my greatest supports during the dissertation process and a great help throughout the data collection period. Without both of your help and support, I would not have been able to complete this research. Thank you for all you both have done.

# Table of Contents

**Abstract iii**

**List of Tables vii**

**List of Figures ix**

## **Chapters**

### **1. Introduction 1**

Background 1  
Problem Statement 3  
Dissertation Goal 6  
Research Question 6  
Relevance and Significance 7  
Barriers and Issues 8  
Assumptions, Limitations and Delimitations 8  
Definition of Terms 10  
Summary 13

### **2. Review of the Literature 14**

Introduction 14  
E-Assessment Security 15  
Authentication Methods 16  
Authentication Weaknesses 17  
    Biometric Authentication Weaknesses 18  
    Webcam Monitoring Weaknesses 18  
    Remote Proctoring Weaknesses 19  
    Continuous Authentication Weaknesses 20  
Continuous Authentication Applied to E-assessment Security 21  
    Presence Verification During E-Assessment 23  
    Identity Verification During E-Assessment 24  
    Authenticating a Student During E-Assessment 25  
Confidence in E-Authentication Security 28  
Trust and Acceptance of E-Authentication for Online Assessment 29  
    Utilization and Effort Concerns 31  
    Privacy Concerns 32  
    Exam Performance Concerns 33  
Theoretical Foundation 36  
Theoretical Model 37  
    UTAUT Model 40  
    Effort Expectancy (EE) 41  
    Attitudes Towards Using Authentication Technology (AT) 42  
    Behavioral Intentions to Use Authentication Technology (BI) 43  
    Perceived Risks (PR) 43  
    Trust in the Technology (TR) 44  
    Privacy Concerns (PC) 45  
Summary 56

<b>3. Research Methodology</b>	<b>58</b>
Research Design	58
Research Method	59
Instrument Development	60
Validity and Reliability	69
Population and Sampling	70
Data Collection	71
Data Analysis	72
Resource Requirements	74
Summary	74
<b>4. Results</b>	<b>76</b>
Overview	76
Sample Demographics	76
Pre-Analysis Data Screening and Validation	78
Data Analysis	80
Findings	82
Proctoring	82
Webcam Monitoring	87
Lock-Down Browser	91
Summary of Results	96
<b>5. Conclusions, Implications, Recommendations, and Summary</b>	<b>100</b>
Overview	100
Conclusions	100
Limitations	112
Implications	112
Recommendations	113
Summary	115
<b>Appendices</b>	
<b>A.</b> Nova IRB Approval	122
<b>B.</b> FIU IRB Approval	123
<b>C.</b> Survey Questionnaire	126
<b>D.</b> Variance Factor Scores	177
<b>E.</b> Equality Covariance Matrices	179
<b>F.</b> Test of Equality of Error Variances	180
<b>G.</b> Reliability Statistics	182
<b>H.</b> Pearson Correlations	183
<b>I.</b> Multivariate Tests (MANOVA)	184
<b>J.</b> Multivariate Tests (MANCOVA)	190
<b>K.</b> Process Procedure Macro (Moderated Mediation Analysis)	193
<b>References</b>	<b>211</b>

## List of Tables

### Tables

1. Authentication Levels 26
2. Authentication Security 27
3. Authentication Instruments 28
4. Related Literature Review Summary 35
5. Constructs in Research with Associated References 46
6. Construct Items with Associated Instrument Source 63
7. Baseline Characteristics of Participants 77
8. Proctoring Authentication MANOVA Results 83
9. Proctoring Authentication Method MANCOVA Results 84
10. Proctoring Authentication Moderated Mediation Results (DV:AT) 85
11. Proctoring Authentication Moderated Mediation Results (DV:BI) 86
12. Proctoring Regression Results 87
13. Webcam Monitoring Authentication Method MANOVA Results 88
14. Webcam Monitoring MANCOVA Results 88
15. Web-Cam Monitoring Authentication Moderated Mediation Results (DV:AT) 89
16. Web-Cam Monitoring Authentication Moderated Mediation Results (DV:BI) 90
17. Webcam Monitoring Regression Results 91
18. Lock-Down Browser Authentication Method MANOVA Results 92
19. Lock-Down Browser Authentication Method MANCOVA Results 92
20. Lock-Down Browser Authentication Moderated Mediation Results (DV:AT) 93
21. Lock-Down Browser Authentication Moderated Mediation Results (DV:BI) 94
22. Lock-Down Browser Regression Results 95



23. Hypotheses Statement of Results H<sub>1</sub>- H<sub>4</sub> 96
24. Hypotheses Statement of Results H<sub>5</sub>- H<sub>7</sub> 98
25. Hypotheses Statement of Results, Correlational Analysis to test H<sub>8</sub> 99

## **List of Figures**

### **Figures**

1. Model for P-I-A goals 23
2. Model for Trust Based E-Authorization System 30
3. Research Model 39
4. Conceptual Research Model With Hypotheses 51
5. Moderated Mediation Path Analysis 97

## **Chapter 1**

### **Introduction**

#### **Background**

In the climate exacerbated by COVID-19 responses, students have been required to adapt to online versions of examinations. The lack of face-to-face interaction or monitoring motivates collusion by students during summative examinations (Ullah et al., 2016). Watson and Sottile (2010) found that students reported that they were four times as likely to engage in academic misconduct in distance learning courses as compared to on campus courses.

Whitelock et al. (2019) claims that there is substantial research to address technological innovations to combat cheating. However, the literature is scarce on assessing the impact of e-authentication systems and whether these technologies would raise student concerns or trust for the e-assessment.

The US congress addresses academic integrity by calling for better student authentication within the Higher Education Opportunity Act of 2008 (Schaefer et al., 2009). The regulation ensures that regional accrediting agencies address the issue of authentication and requires Colleges and Universities to certify that a student who is registered for a course is the same individual completing the course requirements (Brown, 2018; Fisher McLeod, Savage, & Simkin 2016). The legislation also urges implementation of an authentication solution that can verify learner's identity, authenticity, and presence (Lee-Post & Hapke, 2017). Institutions follow the industry standards in terms of information and communication

technology (ICT) management, and some employ multi-factor authentication, but this alone is not sufficient to address the issue of academic integrity, which requires the mapping of learners' physical identities with the academic work they produce. Educational institutions are currently challenged with how to identify online students during e-learning activities, specifically online exams (Fenu et al., 2018). Sabbah, 2017, claims that "e-examination security occupies the highest priority in e-learning solutions, since this module contains the most sensitive data" (p. 158). Consequently, authentication methods are being utilized within e-examination platforms for verifying a student's identity to avoid impersonation attacks. Although it has been found that it is easier to cheat online than in person, little or no attention has been given to providing solutions to cheating in online assessments (Apampa et al., 2010).

"Authentication refers to verifying the identity of a user, device or process, often required before allowing access to a system" (Laamanen et al., 2021, p. 3). The authors imply that this process can be completed at the start of a session or as a continuous process (p. 3). Authentication systems were developed to ensure the practice of integrity is upheld within higher education. Nevertheless, there are several barriers found with authenticating students to avoid the threat of impersonation in online courses. Student authentication is a major challenge in online learning within higher education institutions and improving learner authentication is of critical importance due to the risk of possible impersonation (Laamanen et al., 2021). However, impersonation attacks are difficult to mitigate in a remote online environment (Ullah et al., 2018). Universities have spent time and resources ensuring that students are properly authenticated within the online learning environment. Nonetheless, impersonation attacks are a reality in many online learning activities. Although it is challenging to track collusion attacks after the completion of a test; mitigation of such attacks may be necessary to increase the confidence of stakeholders (Ullah et al., 2016). Although systems may be protected from

impersonation attacks, student attitudes and intentions to use the system may be affected. Authentication methods should provide the highest levels of security against impersonation attacks, but the e-assessment system should be easy to use, should also be non-invasive, and not diminish a user's privacy (Ullah et al., 2018). Researchers suggest that "the way to minimize cheating or impersonating during online exams, is to develop a continuous authentication system on the online exam application that can validate the suitability of the examinees and identify participants who are cheating during the exam" (Aisyah et al., 2018, p. 171). Continuous authentication is a method applied to ensure that the user remains the same throughout a certain period (Peris-Lopez et al., 2018). However, there may be problems with employing continuous authentication approaches to secure e-assessments.

### **Problem Statement**

Although authentication methods are deemed necessary, there are several limitations to this technology, including low levels of security and efficiency in mitigating impersonation attacks. Studies have shown that single factor authentication can only prevent impersonation at initial login and thereafter a next level solution such as continuous authentication is needed (Fenu et al., 2018; Lee-Post & Hapke, 2017). Albeit "continuous authentication itself, cannot entirely eliminate cheating in online learning environments and no solution can fully eliminate cheating" (Moini & Madni, 2009, p. 474). In essence, although continuous authentication approaches are utilized to secure online exams against impersonation attacks there may be student concerns with employing this approach. Employing authentication methods to reduce impersonation attacks should provide high levels of security while preventing exam disruptions and should consider privacy concerns (Fenu et al., 2018; Ullah et al., 2018).

Continuous surveillance may cost examinees their privacy (Fenu et al., 2018; Naveen, et al., 2018). The use of biometrics also has privacy and legal implications as facial images, and fingerprints can be taken without knowledge or consent unveiling a student's identity (Moini & Madni, 2009). Proctoring, for example, has been found to have high continuous identity assurance as students are monitored throughout the process after being authenticated (Amigud et al., 2018). However, research confirms that remote invigilation can develop privacy and data protection issues (Amigud et al., 2018; Brown, 2018; Bristol, 2017; Chou & Chen, 2016; Hylton et al., 2016; Lilley, Meere, & Barker, 2016). Moreover, students are concerned about invasion of privacy with third party vendors and their ability to track their actions on the internet (Brown, 2018). Students may also be concerned that the authentication process can limit their exam performance.

Lilley et al. (2016) found a major drawback to be that students exhibit stress levels during remote proctoring. The authors found that examinees were primarily concerned about their security and privacy during remote proctoring and the extent to which the process would intrude on their privacy and impact negatively on the testing experience. Participants also had initial concerns about data protection and the impact of how feeling watched may affect their online experience (Lilley et al., 2016). Findings in the study suggested that most students found that remote proctoring “did not affect the assessment experience” (p. 1). However, the research showed that participants who did not support the use of the technology commented that “the authentication process made students feel like they are being watched and that it took too long to authenticate resulting in some assessment anxiety” (Lilley et al., 2016, p. 3). Essentially, students conclude that authenticating during e-assessments may in effect, take a great deal of effort.

The use of the examination software during e-assessments may be concerning to students due to the effort asserted during the authentication process. An exemplary model for authentication assurance should be transparent without affecting the normal student activities (Fenu et al., 2018). Prakash and Mukesh (2014) cited that hard biometric such as fingerprint or face recognition checking can be inconvenient to the user. Further, Flior and Kowalski (2010) and Sabbah (2017) suggested that authentication methods can be intrusive. Moreover, Naveen et al. (2018) asserts that proctoring surveillance can cause uneasiness to the students.

Succinctly, the literature suggests methods for increasing efficiency and security of continuous authentication (Apampa et al., 2010; Sabbah, 2017). The literature also covers methods for increasing levels of security to reduce impersonation attacks (Moini & Madni, 2009). Although there is an ample amount of literature that addresses how to apply e-assessment security through continuous authentication methods to mitigate impersonation attacks, it is important to consider student attitudes concerning authenticating during an exam and whether their intentions to use the exam system is affected. In essence, it is unclear whether student attitudes and intentions to use the exam system is related to privacy concerns, the amount of effort expected to authenticate during the exam or exam performance expectations. Universities spend time and money on authentication methods to ensure confidence in e-examination security; however, the literature is clear that students may have concerns about authenticating during an examination.

Colleges and universities subscribe to authentication approaches to secure examinations against impersonation attacks, however, student attitudes and intention to use a system that employs continuous authentication methods may be overlooked. Thus far, researchers are dedicated to examining whether authentication methods are effective against protecting e-assessment systems from impersonation attacks. Essentially, a considerable disparity is to

understand whether the authentication system would increase student concerns on e-assessment as the literature is limited on the impact of e-authentication tools across distinctive end users since it is not a widespread practice (Okada et al., 2019). It was worth investigating student attitudes and their intentions to use technologies that apply continuous authentication techniques. Understanding this problem is important for the overall success of the university metrics in graduating and retaining students.

### **Dissertation Goal**

Using the Unified Theory of Acceptance and Use of Technology Model (UTAUT), the goal of this study was to determine the relationship between student attitudes and intention to use e-examination software that applies continuous authentication methods to mitigate impersonation attacks. A descriptive study was conducted to better understand student attitudes and acceptance for continuous authentication methods which secure e-examinations against impersonation attacks. Considering the UTAT model, a framework was established to understand the relationship between student attitudes and intentions to use the e-assessment system and their concern for privacy, their expectations for performance on the exam and their concern that it may take a substantial amount of effort to use the exam system. This study seeks to address a pivotal research question that explores key insights to using continuous authentication methods. The following is the primary research question that will be addressed.

### **Research Question**

Applying a framework from UTAUT model, the following primary research question was examined: How does student concerns for continuous authentication methods applied to



mitigate impersonation attacks affect students' attitudes and intentions to use the technology during an e-exam?

### **Relevance and Significance**

COVID-19 has drastically changed the way higher education institutions operate by abruptly enforcing distance learning to protect students, faculty, and staff (Kharbat & Abu Daabes, 2021). Understanding student perceptions of authentication tools within the online examination experience is limited. In addition, Laamanen et al. (2021) posits that understanding acceptability of e-authentication systems should further be explored. This study focused on online learning within the higher education context. The goal was to shed light on how authentication intended to secure e-assessment against impersonation attacks during online e-examinations may impact student attitudes during the exam experience and their intentions to use the e-exam system. This study is relevant because the problem may affect students who are required to utilize authentication methods to confirm their identities and to protect e-assessments against impersonation attacks. Instructors can also be affected as final grades will not reflect a student's effort in preparing for an exam. In addition, a reduction in student retention may become evident through graduation metrics. More specifically, examining student attitudes for e-assessment reassures the quality assurer and faculty that applying authentication methods can be both secure and will also certify whether students trust the authentication process. Creating student trust for continuous authentication seems to be an arduous task. Addressing the problem uncovers a model for enhancing the student experience while securing an e-exam against impersonation attacks. With the growth of new technologies and more students taking online and remote courses, demand for continuous authentication approaches may increase. This research adds to the body of knowledge by uncovering current

solutions for authenticating e-exams and uncovering the impact this may have on the student exam experience with the purpose of shedding light on whether best practice strategies are necessary. The study sampled from a four-year university and can be generalized to similar universities of size and structure as the diverse student body at consists of 56,000 students.

### **Barriers and Issues**

There were several barriers and obstacles faced when investigating this study. One obstacle expected was reliance on participation in the study. Finding solutions for authenticating e-exams can be inherently difficult to solve as it requires recruitment, retention, and participation of research participants. It was expected that recruiting participants to complete the survey instrument percentage would be an arduous task. Gathering and analyzing data to understand student attitudes was also expected to be a difficult task as it requires a certain completion rate to run the appropriate statistical analysis. It was also considered that the types of continuous authentication methods used to identify students during an exam would be limited to certain technologies. Obtaining the required permission to recruit research participants and collect data was also an expected barrier since it required permission from the Institutional Review Board (IRB) of two major universities for participation of human subjects. There is also a chance that although the finding in this research may be beneficial, it may not be considered a useful practice implemented by faculty and the quality assurance team.

### **Assumptions, Limitations and Delimitations**

Assumptions serve as a foundation of a proposed research and constitute “what the researcher assumes to be true” (Leedy & Ormrod, 2010, p. 5). Moreover, assumptions can be

viewed as something the researcher accepts as true without concrete proof (Ellis & Levy, 2009). The following assumptions were considered for this research. It was assumed that there will be an ample sample of research participants who have experience with authenticating while taking online summative e-assessments. Participants in the study were required to have experience in using one or more of the continuous authentication schemes outlined in this study. It was essential for research participants to easily be able to recall their experiences with the use of continuous authentication during an e-assessment. Participants in the study should also have had familiarity with using a computer and accessing the survey instrument. Finally, it was assumed that students would log onto the Sona system to complete the survey instrument.

Cresswell & Cresswell (2018) defines limitations as potential weaknesses within a study. Ellis & Levy (2009) affirms that limitations may be viewed as a threat to the internal and external validity of the study (p. 332). The authors point out that two possible limitations in most studies include the fact that participants recruited for the study may withdraw at any point and this may result in a misrepresentation of the sample population. In this regard, due to time constraints during this research, the investigation was based on a cross-sectional study. The implication is that data was collected at one point in time from invited participants.

Delimitations refer to “what the researcher intends to do and what is not going to be done in the research” (Leedy & Ormrod, 2010, p. 57). In the scope of this research, the study focused on students enrolled from the freshman to senior level in a university. Participants were to be chosen from a fully online course whereby the faculty chooses to utilize authentication methods to verify students during a summative e-assessment. The study was required to be constrained to examining student attitudes about trust for authentication technologies, privacy concerns, expectations of exam performance, and utilization of the

system when authenticating during an e-examination. The following section reviews a list of terms relevant to this research.

### **Definition of Terms**

The following are defined terms for this study:

1. Attitude – reflects the degree of positivity or negativity that a person feels towards an object (Lavrakas, 2008). Within the context of e-learning attitude refers to “an individual’s positive or negative feeling about performing a target behavior” (Abdou & Jasimuddin, 2020, p. 42).
2. Authentication – authentication includes two principal elements to check for impersonation instances: identification and verification (Levy & Ramim, 2009).
3. Behavioral Intentions – Within the context of e-learning, this term refers to the “intent for the learners to employ e-learning systems and involves persistent use from the present to the future” (Salloum et al., 2019, p. 514).
4. Biometric Authentication – biometric authentication is the security manner of identifying a real person and relies on the unique person’s biological characteristics (Alkhateeb, 2020).
5. Bimodal Biometrics – bi-modal authentication uses biometric equipment such as a finger-print scanner to statistically authenticate the user (Gathuri et al., 2014).
6. Bi-modal Authentication – uses biometric equipment such as a finger-print scanner to statistically authenticate the user (Gathuri et al., 2014).
7. Dynamic Authentication – users are validated at any moment during the interaction with the system (Niinuma et al., 2010).

8. Effort Expectancy – The extent to which a user perceives using the system is a free effort (Chiu & Wang, 2008).
9. Electronic Authentication (or e-authentication) – “the process of establishing confidence in the user identities” (Moini & Madni, 2009, p. 471).
10. Face Recognition – “one of the most significant applications of image understanding, this task does not solely on identity but is also influenced by illumination and viewpoint (Zhang & Samaras, 2004, p. 1 ).
11. Formative Assessment – formative assessments are built to test the student’s acquired skills while continuously tracking their progress (Gathuri et al., 2014).
12. Identity – identity reflects uniqueness to answer the question “who are you?” to distinguish one student from another (Apampa et al., 2010).
13. Multimodal Biometrics – utilizes a number of different biometric identifiers like face, fingerprint, hand-geometry, and iris can be more robust to noise and alleviate the problem of non-universality and lack of distinctiveness” (Alkhateeb, 2020, p. 259).
14. Perceived Ease of Use – The degree to which a person believes that the system would be a free effort (Venkatesh et al., 2003).
15. Perceived Risk – “Uncertainty that affects people’s confidence in their decisions” (Im et al., 2008, p. 2).
16. Perceived Usefulness – The degree to which using an innovation is perceived as being difficult to use (Venkatesh et al., 2003).
17. Performance Expectancy – Perceptions of the end-user on improving (or declining) performance and increasing (or decreasing) efficiency achieved through use of the e-learning technology (Abdou & Jasimuddin, 2020).
18. Presence – presence checks if the user is always present (Apampa et al., 2010).

19. Privacy Concerns – The perception of a user regarding their ability to monitor and control their information during an online transaction (Escobar-Rodriguez & Carajal-Truillo, 2014).
20. Proctoring – students are monitored throughout the exam process by a human invigilator after being authenticated (Amigud et al., 2018).
21. Summative Assessment – summative assessments look at student achievements and are measured in grades (Gathuri et al., 2014).
22. Unimodal Biometrics – “unimodal biometric systems make use of a single biometric trait for user recognition” (Alkhateeb, 2020, p. 259).
23. Static Authentication – user verification is identified once (Niinuma et al., 2010).
24. Multi-authentication – seek to combine two or more of the above methods to overcome the limitations of a single method” (Levy et al., 2011, p. 105).
25. Trust – Generating a sense or perception of certainty (Miltgen et al., 2013).
26. Type A Impersonation Threat – when an impersonator is allowed by the testing agent to take an exam, in some cases in exchange for monetary purposes (Gathuri et al., 2014).
27. Type B Impersonation Threat – when a legitimate student passes his information on to a fraudulent party to get help on the exam.
28. Type C Impersonation Threat – where a valid student logs in and allows the impersonator to continue taking the exam (Gathuri et al., 2014).
29. Type D Impersonation Threat –the real examinee is taking the exam, but another person assists him for correct answers (Sabbah, 2017, p. 162).
30. Video monitoring –video monitoring allows an administrator to view recorded video footage at any point (Levy et al., 2011).

## **Summary**

Chapter 1 explained how continuous authentication methods applied to e-exams can protect against impersonation attacks but can also cause concerns and trust issues for the examinee. It is essential to consider the user's attitudes and intentions to use the exam software to ensure that students have a comfortable experience that will not affect their attitudes towards privacy, performance expectations and effort expectations in using the system. Information systems research can benefit from an inquiry on whether continuous authentication approaches applied to increase e-assessment security can affect student attitudes and intentions to use the exam system due to performance expectancy, effort expectancy and privacy concerns. The following is an exploration of the literature which connects the background and theory for this study.

## Chapter 2

### Review of the Literature

#### Introduction

The literature review evaluates the types of continuous authentication being used to secure e-assessments against impersonation attacks and uncovers levels and methods of security applied to safeguard the e-examination. Particularly, it was worth exploring how confidence for authentication security is established and whether the application of methods to secure a system may impact a student's exam experience. Other information extracted from the literature supports the claim that students may be concerned about authenticating during an e-assessment due to privacy concerns, effort in using the system, and performance expectations. In essence, the exploration of literature defines the scope of this research.

Ullah et al. (2016) indicates that “an online exam is a critical asset in the context of online learning” (p. 1). However, online assessments are subjected to several security threats including impersonation threats. Gathuri et al. (2014) outlined and defined the different types of assessments being utilized within online learning. For example, electronic assessments (or e-assessments) are delivered and displayed through a computer screen over the internet. Formative assessments are built to test the student's acquired skills while continuously tracking their progress, whereas summative assessments look at student achievements and are measured in grades. Diagnostic assessments identify strengths and weaknesses or learning challenges. Because summative assessments are tied to grades, students may be pressured to invite an



impersonator to assist them with the e-assessment. In e-assessments impersonation attacks are considered a major concern and is realized as a great risk by the academic community (Apampa et al., 2010). This study focused on continuous authentication methods that are implemented online to mitigate impersonation on summative e-assessments. The literature reviews authentication strategies utilized to protect e-assessments against impersonation attacks and further addresses student concerns for privacy, their expectations for performance on the exam, and their expectations for exerting effort to authenticate during the examination.

### **E-Assessment Security**

Ullah et al. (2016) outlines major security threats to online exams within the context of collusion. The authors point out that “collusion occurs when a student invites a third-party collaborator to impersonate or aid a student to take an online test.” The researchers affirm that intrusion attacks happen without the knowledge of the student whereas non-intrusion attacks are welcomed attacks that come from a legitimate student who colludes with a third party. This study focuses on authentication applied to mitigate non-intrusion attacks. The authors emphasize that impersonation attacks occur when an online examination is taken by a third-party impersonator, the attacks are pre-planned and consensual. In contrast, abetting attacks involves a student who takes aid from a third party during an examination. This research looks at concerns for authentication methods that mitigate against impersonation incidents and/or abetting attacks. Gathuri et al. (2014) categorized impersonation threats into three types of attacks as outlined further. Type A impersonation threat is when an impersonator is allowed by the testing agent to take an exam in some cases in exchange for monetary purposes. Type B occurs when a legitimate student passes his information on to a fraudulent party to get help on the exam and type C is where a valid student logs in and allows the impersonator to continue

taking the exam. Recently added to the research is a Type D impersonation threat whereby the real examinee is taking the exam, but another person assists him for correct answers (Sabbah, 2017). The analysis emphasizes continuous authentication approaches used to prevent B, C and D type impersonation threats. To ensure e-assessment security, authentication methods are used to check for impersonation attacks during log in and verification, however there are drawbacks.

### **Authentication Methods**

Authentication includes two principal elements to check for impersonation instances such as identification and verification (Levy & Ramim, 2009). User authentication can be static, whereby verification is identified once or dynamic, where users are validated at any moment during the interaction with the system (Niinuma et al., 2010). E-authentication approaches have been categorized into five main schemes including proctored-only, unimodal biometrics, bi-modal biometrics, video monitoring and biometrics with webcam monitoring (Gathuri et al., 2014). In online environments, the authentication methods are applied in the following ways.

Human invigilators are used to monitor students in proctored-only formats. Unimodal authentication is used during log-in and may require a username and password. Bi-modal authentication uses biometric equipment such as a finger-print scanner to statistically authenticate the user (Gathuri et al., 2014). Biometric systems recognize physical characteristics of a person, such as fingerprint, handwriting patterns, or keystroke patterns (Levy, et al., 2011). Video monitoring allows an administrator to view recorded video footage at any point. Biometrics and webcam monitoring first authenticates a student then begins monitoring via webcam. Multi-authentication techniques combine several of the above

methods to overcome the limitations of a single method (Levy et al., 2011). In comparison, continuous authentication constantly monitors and authenticates the student throughout a session and is used to mitigate impersonation threats. Impersonation threats are associated with the exclusion of presence verification throughout the test session (Apampa et al., 2011). Applying continuous authentication to e-assessments can verify student identity to reduce instances of impersonation but may have weak spots. The literature subsequently addresses authentication weaknesses as it pertains to securing systems against impersonation threats.

### **Authentication Weaknesses**

Existing continuous authentication schemes utilize hard biometrics such as fingerprint or face recognition, which is inconvenient to the user (Prakash & Mukesh, 2014). Drawbacks to the authentication approaches according to Flior and Kowalski (2010) and Sabbah (2017) includes the following. Knowledge factors can never be trusted for continuous authentication, and if the password is given away then the security can be cancelled. Regarding ownership factors, a token is requested and can be passed on to others and tokens requested at login cannot be trusted for continuous authentication. Finally, Flior and Kowalski (2010) and Sabbah (2017) suggested that the inheritance factors can be costly, unreasonably intrusive, expensive, and difficult to implement. Existing methods of continuous authentication may include a combination of multi-modal biometrics, invigilation, video monitoring and password verification (Apampa et al., 2011). Student authentication is a major challenge in higher education institutions within the context of online learning as online impersonation is a threat (Laamaen et al., 2021). Therefore, a plethora of authentication approaches have been adopted to mitigate this issue. Each method of authentication implemented includes shortcomings that may be of concern to examinees as well as quality assurers. The following will review the

different types of authentication methods used to mitigate impersonation attacks during e-assessment, will outline weaknesses for each method and will identify how the authentication approach may cause concern for students.

#### *Biometric Authentication Weaknesses*

Detecting signs of liveliness could be a difficult problem and detection mechanisms can be intrusive, costly, and the verification process can be lengthy (Moini & Madni, 2009). According to Apampa et al. (2010), biometric authentication has a strong potential to be subjected to Type C impersonation threat. The use of biometrics can have privacy and legal implications as biometrics can be publicly observable and there are also concerns of how this information is stored (Moini & Madni, 2009). Apampa et al. (2010) observed that “any solution of bimodal biometric authentication is insufficient to minimize threats to e-examinations although threats can be minimized to a certain degree based on the type of biometrics adopted”. Submitting live samples of biometric data to the system has problems of detecting signs of liveliness and therefore biometrics do not provide absolute identification (Moini & Madni, 2009). Other limitations found are that biometric data cannot be revoked, cancelled, reissued if compromised and does not offer cancellation of actions. In addition, biometric authentication can be costly including hardware, software and training of staff and students (Ullah et al., 2012). Video monitoring is another form of detecting and monitoring an examinee (although this method also has shortcomings).

#### *Webcam Monitoring Weaknesses*

Video monitoring is susceptible to Type B impersonation threats (Apampa et al., 2010; Gathuri et al., 2014). Apampa et al. (2011) asserts that “type B impersonation threat can occur as a result of the strength or weakness of the authentication method adopted” (p.3). The authors

also find that this form of authentication, even coupled with a password at entry is also susceptible to types A and C impersonation threats as well. A major disadvantage is dependence on the invigilator as they may look away or get distracted while reviewing footage or monitoring a student (Apampa et al., 2016). Another disadvantage found is the administrative task of having to review videos which may prove inadequate due to time and can become a jarring task (Apampa et al., 2010; Gathuri et al., 2014). Due to the overwhelming nature of this daunting task, instances of collusion can be overlooked. Video monitoring coupled with biometric webcam monitoring can also be subjected to a type C impersonation attack (Apampa et al., 2010). Remote proctoring is similar to video monitoring, except this method employs a human invigilator to oversee the monitoring process.

#### *Remote Proctoring Weaknesses*

Remote proctoring has proven to be a popular solution to authenticate students during online examinations as a third-party is hired to identify the examinee throughout an e-assessment. Nevertheless, privacy and security concerns reported by students include being viewed by a stranger and sharing living environment, showing personal ID to a stranger, giving a stranger remote access to their personal computer, and the need for ensuring that proctoring services are adhering to data protection and privacy laws (Lilley et al. 2016). Hilton et al. (2016) suggested that proctoring technology solutions are dependent on third party providers, which is an issue that raises concerns about privacy and security if proctoring services are not properly contracted with the home institution. Moreover, “privacy concerns have been highlighted by the lawsuit filed against the Pennsylvania school district for activating webcams of school laptops within the homes of students and capturing video images” (Hylton et al., 2016, p. 55). Cifuentes and Janney (2016) warned that when storing students’ data on a third-party vendor’s cloud-based server, network security officers, and administrators should be

aware that sensitive data will be stored on the vendor's facilities. To challenge the referenced weaknesses in e-assessment security, continuous authentication assurance is applied to mitigate impersonation attacks. However, this method also has deficiencies.

### *Continuous Authentication Weaknesses*

Ullah et al. (2018) stated that academic dishonesty has been widely researched as a major security threat due to vulnerable authentication approaches. It addressed within the research, that current methods of authentication do not offer a rigorous continuous approach for identifying users (Amigud et al., 2018; Amigud et al., 2017; Kang & Kim, 2015; Lee-Post & Hapke, 2017). This leaves instructors with the task of applying various technologies to identify users to align learner identities with their academic work (Amiguid et al., 2018). Further, it is unclear what authentication methods are best combined to maintain user friendliness while securing e-assessments against collusion or impersonation attacks. Although there are successful ways for identifying students through continuous authentication methods, Amigud et al. (2017) pointed out that combinations may cause gaps or blind spots and may miss fully screening and identifying students. Moini and Madni, (2009) informs that "Certain types of biometrics allow users to be re-authenticated repeatedly (or authenticated continuously) without interfering with user activities" (p.471). Naveen et al. (2018) proposes a system for authentication through palm-print recognition, in combination with username and password for initial authentication and webcams for continuous surveillance. Yet, a major drawback to the system is that the continuous surveillance might cause uneasiness to the examinee. The student may also feel uneasy about violation of their privacy. According to Miltgen et al. (2013) users feel fearful and hesitant or uncomfortable with biometric authentication systems because they perceive them as potential infringements on their privacy. Further, with a combination of the biometrics and webcam approach, security may be breached

when the student authenticates and then turns the view of the webcam to an impersonator (Gathuri et al., 2014). Several combinations of these proposed authentication methods can also cause disruption or limit the utilization of the examination software compelling students to exert a certain amount of effort to authenticate during the exam. Studies have been dedicated to confidence in e-authentication or “the process of establishing confidence in user identities electronically presented to a system” (Moini & Madni, 2009, p. 470). However, consideration of student attitudes and acceptance towards application of authentication methods is limited in the research (Kharbat & Abu Daabes, 2021; Laamaen et al., 2021). Although authentication methods have been found to have weak spots, these approaches are nevertheless applied to secure e-exams against impersonation attacks. However, an optimal method to authenticating should include high security assurance for the e-assessment and should also consider student concerns for privacy, performance expectations and effort in using the system as addressed within the literature.

### **Continuous Authentication Applied to E-assessment Security**

Moini & Madni (2009) states that one time authentication approaches are highly vulnerable to fraud and attacks, whereas schemes for continuous authentication mechanisms improve the reliability and confidence in the authentication process. The authors defined electronic authentication, or e-authentication, as the process of establishing confidence in the user identities. Continuous authentication approaches are required since caution should be taken in online exams and e-examination systems should verify an examinee is the actual student (Sabbah, 2017). Apampa et al. (2010) advises that “one of the main characteristics of an e-assessment system is the ability to securely provide an examination which is delivered to the correct student” (p.136). The authors point out that user security plays a vital role in e-

assessments but poses two challenges which are identity and authentication. (Apampa et al., 2010). The ability of the students to provide the correct responses will give the security system an assurance that the correct examinee is taking the exam based on identity and authentication (Apampa et al., 2010). An assurance method to confirm correct user security during online tests is “to combine the presence goals and continuously authenticated presence with the existing identity and authentication security goals” (Apampa et al., 2010, p. 140). Students should be required to satisfy continuous authenticated presence, identity, and authentication security goals prior to and during the online test (Apampa et al., 2009, p. 2). Security goals employed to ensure that hardware, software, and data assets are not compromised, includes three components based on the C-I-A model (C-confidentiality, I-integrity, and A-availability) (Apampa et al., 2010; Sabbah, 2017).

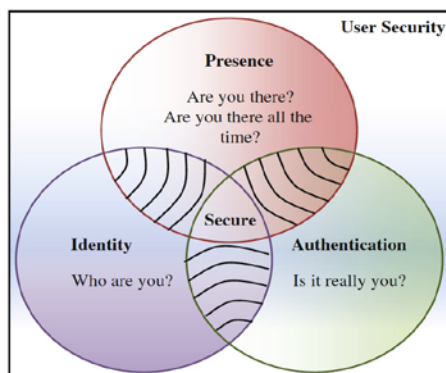
Authentication methods are supposed to satisfy all three C-I-A goals to ensure security of critical assets. However, in terms of detecting impersonation through continuous authentication, other goals may be necessary to confirm assurance in e-assessment security. Presence, identity, and authentication (P-I-A) create a model for assurance in the presence, identity and authentication needed to continuously identify the student. “P-I-A goals takes into account the student’s presence, continuously authenticated presence, their identity, and their authentication” (Sabbah, 2017, p. 161). For confidence in e-assessment security to exist, continuous authentication assurance requires that the presence, identity, and authentication (P-I-A) goals have been met as suggested by Apampa et al. and Sabbah. P-I-A goals ensure the student’s presence and identity is continuously authenticated throughout the e-assessment (2017). Meeting the P-I-A goals yields confidence in e-assessment security. P-I-A goals are respectively implemented to secure an e-assessment system against impersonation attacks during an examination. However, if continuous authentication



methods scan to determine presence, identity and authenticity of a user, the system should be flexible and scalable enough to accommodate users through the process of verification and re-verification (Ryu et al., 2021). The continuous authentication system should also ensure confidentiality of private data stored while protecting our personal information through privacy preservation methods (Hernández-Álvarez et al., 2020). The P-I-A model for establishing continuous authentication as defined by Apampa et al. (2010) and Sabbah (2017) follows in Figure 1.

**Figure 1**

*Model for PIA Goals for User Security*



*Note.* The image represents a model for presence, identity, and authentication to ensure e-assessments user security. From “Security of online examinations” by Y.,W. Sabbah, 2017, *Data Analytics and Decision Support for Cybersecurity. Data Analytics.* p.161 ([https://doi.org/10.1007/978-3-319-59439-2\\_6](https://doi.org/10.1007/978-3-319-59439-2_6)). Copyright 2018 by Springer International Publishing.

#### *Presence Verification During E-Assessment*

Apampa et al. (2011) associated impersonation threats in e-assessment environments to the exclusion of presence verification throughout the test session. Therefore, “there is a need to

verify the presence of an authenticated student beyond the initial login procedure” (Apampa et al., 2011, p. 3). The authors suggested several approaches to presence verification during summative e-assessments including using an invigilator or proctor, although this method has limitations to verifying a student’s presence (Apampa et al., 2010). Unimodal active biometrics used in summative e-assessments such as fingerprint and face recognition are said to enhance security and minimize impersonation threats and can achieve presence verification through continuous re-scan of a student’s fingerprint throughout the test session (Apampa et al., 2011). However, this method is considered as interruptive or distracting to the students’ concentration (Apampa et al., 2011). In addition, unimodal biometrics, such as face recognition, which are considered passive, are used in e-assessments to verify continuous authentication, although this method requires a large amount of processing power (Apampa et al., 2011). In summative assessments, continuously authenticating a student’s face is expensive, impractical and requires continuous frontal face images for successful authentication (Apampa et al., 2011). In this case, the student may be constrained to not stare away from the focus of the camera which might make them uncomfortable. Apampa et al. (2010) asserts that after a few attempts of being unable to capture the student’s face, the consequence will be an interruptive re-authentication request or an automatic log out.

#### *Identity Verification During E-Assessment*

Identity reflects uniqueness; hence an e-assessment security system requires a student to answer the question “who are you” to distinguish one student from another (Apampa et al., 2010). A username is typically employed to identify users during the e-assessment. However, this can be easily shared or stolen, and correctness of a student should not be assumed based on only identification, as additional proof is required to show that the identify claimed belongs to the owner who stored the information (Apampa et al., 2010). Therefore, the student must also

be authenticated. As verification of identity asks the question; “who are you”, authentication asks the question “is it really you” (Apampa et al., 2010). Therefore, authentication methods are needed to check the student’s identity.

### *Authenticating a Student During E-Assessment*

Authentication methods in the context of e-examination can be classified into three factors; something the user knows such as a password, ownership factors such as something the user possesses, or inheritance factors for instance, something the user is or does (Apampa et al., 2010; Sabbah, 2017). E-assessment security depicts a username as a form of identity and one or more of the above authentication methods to prove the claimed identity to ensure that the correct student is taking the exam (Apampa et al., 2010). The U.S. Federal agencies (OMB) identified four levels of e-authentication in terms of the consequences of authentication errors and misuse of credentials signifying “the more serious the consequence, the higher the level of assurance required” (Moini & Madni, 2009, p. 470). Furthermore, Moini & Madni (2009) stated that, “the more authentication factors employed, the stronger the authentication” (p. 479). Level 1 includes no identity proofing, where there is little or no confidence in the identity based on a weak password and is very vulnerable to eavesdropping. Level 2 is the single-factor approach such as in the case of unimodal authentication strategies. The use of better passwords is found at this level, but this is still vulnerable to phishing, social engineering, and other attacks. Level 3 is based on the two-factor authentication approach, where password and soft crypto token or one-time password device is required which produces a high confidence in identity and assurance in avoiding phishing attacks. The authors point out that level 4 requires “identity proofing, hard crypto tokens and utilization of crypto binding of authentication and data transfer” (p. 471). Level 4 is said to have a “very high confidence in asserted identity” and

is required for more serious consequences of authentication errors (p. 471). Authentication levels as defined by the authors can be found in Table 1.

**Table 1**

*Authentication Levels*

Level	Description
Level 1:	No identity proofing (little confidence in asserted identity; weak password are allowed and is vulnerable to eavesdropping)
	Single factor using better pass
Level 2:	words (some confidence in asserted identity, but still vulnerable to phishing, social engineering, and other attacks).
Level 3:	Two-factor e.g., password and soft crypto token or one-time password device (high confidence in asserted identity; phishing attacks shouldn't get master authentication secret)
Level 4:	In-person identity proofing requiring hard crypto tokens and utilizing crypto binding of authentication and data transfer (very high confidence in asserted identity)

*Note.* The above table highlights authentication levels to show the higher the level of authentication, the higher the confidence in securing the system against impersonation attacks.

From “Leveraging biometrics for user authentication in online learning: A systems perspective.” by Moini, and Madni, 2009, *IEEE Systems Journal, Systems Journal, IEEE, 3(4)*, p. 470. Copyright 2009 by IEEE.

According to research conducted by Aisyah et al. (2018), authentication methods used for online tests can be analyzed based on both level of security and effectiveness of each method to minimize cheating through impersonation and can be categorized as knowledge based, possession based and biometric based as found in Table 2. In essence, P-I-A goals, the level, and effectiveness of authentication methods applied to mitigate impersonation attacks, are defined within the literature as techniques for increasing confidence in security on e-assessments. As shown in Table 2, a comparison of authentication methods is presented based

on the strength of security and privacy. These security approaches are utilized based on the type of authentication methods used to mitigate impersonation attacks during e-exams.

**Table 2**

*Authentication Security*

Indicator	KBA	PBA	Biometrics	Explanation
User Credentials are easy to share.	✓	✓	-	This is indicated as a security weakness of KBA method. User credentials of KBA can easily be shared. Examinees can share login credentials and personal information to third parties who are trusted to replace students working on online exams. This is indicated as security weakness of PBA method. User credentials of PBA. Method easy to share, PBA objects can be easily transferred and used for cheating.
Easy to hack and duplicate	✓	-	-	
Privacy Issues	-	-	✓	

*Note.* Methods applied to indicate confidence in security, or the effectiveness of knowledge

based, possession based and biometric based authentication. From “Development of

continuous authentication system on android-based online exam application” by S. Aisyah and

L. B. Subekti, 2018, *Proceedings of the International Conference on Information Technology*

*Systems and Innovation*, p. 172. Copyright 2018 by IEEE.

Some examples of knowledge based, possession based, and biometric based authentication can be found in Table 3. To ensure security, continuous authentication can employ any of these three approaches and a combination of these technologies. Examples for each category are presented within the table. These common authentication mechanisms could

be applied to e-exams based on the type of technology. The authentication methods applied can vary based on the levels of strength necessary to ensure that the system is secure from impersonation attacks.

**Table 3**

*Authentication Instruments*

<b>Knowledge based</b>	<b>Possession Based</b>	<b>Biometrics</b>
Password	Smart Card	Facial Image
Username	Security Card	Voice
Code	ATM Card	Keystroke rhythm
Pin	Mobile Phone	Fingerprint
Pattern		Signature

*Note.* Examples of common e-authentication instruments. From “Acceptability of the e-authentication in higher education studies: views of students with special educational needs and disabilities,” by Laamanen et al. 2021, International Journal of Educational Technology in Higher Education, p. 4. Copyright 2021 by The Authors.

### **Confidence in E-Authentication Security**

Based on the literature, the P-I-A model is recommended during continuous authentication to ensure that a students’ presence and identity is verified within the testing environment (Apampa et al., 2010; Sabbah, 2017). P-I-A goals are implemented to confirm that the system cannot be compromised by impersonation threats during e-assessments. The P-I-A model should be an integral part of continuous authentication assurance. According to the literature, if P-I-A standards are applied correctly then a system should be secure and may not be compromised, making for a strong standard of confidence in continuous authentication

assurance (Sabbah, 2017). In addition, the security levels can confirm confidence in the asserted identity of an individual. Further, authentication methods used for online e-assessments can be analyzed based on the effectiveness of each method to minimize cheating through impersonation. Collectively, these approaches can result in distinctive levels of confidence in e-assessment security. However, these authentication approaches may also raise student concerns.

Although quality assurers may use a combination of continuous authentication methods to secure e-assessments against impersonation attacks, students may have concerns and trust issues when authenticating during an e-assessment. Student concerns and trust for the authentication process and gaps regarding this issue subsequently follows.

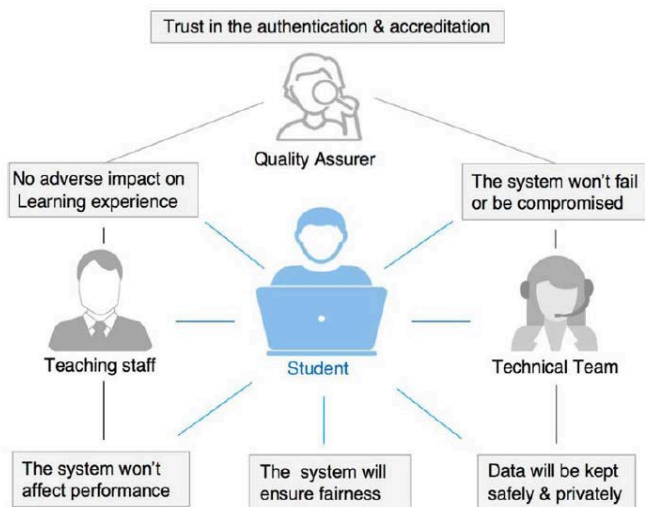
### **Trust and Acceptance of E-Authentication for Online Assessment**

It is important to study acceptability of e-authentication tools as users may deny utilizing this technology (Laamaen et al., 2021). Okada et al. (2019) set out to investigate student attitudes towards the use of e-authentication in online assessments and found a broad positive acceptance of trust in authentication for online assessment by both male and female students. The authors examined student attitudes and experiences of a system used to check authentication and authorship of e-assessments and uncovered privacy and trust issues for e-authentication tools used during online assessments. They also found utilization issues that included technical problems faced by students when using the authentication system. Further findings show that student concerns for the e-assessment might impact student performance on the exam. Okada et al. (2019) asserts that “a considerable gap found within the literature is to understand whether the use of e-authentication systems would increase student trust on e-assessment and to further understand student acceptance of e-authentication systems” (p. 861).

The research by the authors suggests the following model found in Figure 2 for applying authentication which considers a student's attitudes on privacy, effort in utilization of the system, and student expectations for performance during online assessment. A framework for establishing privacy-trust places the student at the center of the authentication experience and requires action from the quality assurer, the technical team, and the teaching staff to ensure that the student trusts the system (Okada et al., 2019). The authors advised that data should be kept safe and private, the system should not affect performance and should not fail or be compromised when used. This research on student trust for authentication technology synthesizes and extracts three important constructs that will be examined within this research.

**Figure 2**

*A Model for Trust-based e-authorization system*



*Note.* Depiction of a model for trust-based adapted e-authentication system. From “ E-Authentication for online assessment: A mixed-method study,” by A. Okada et al, 2019, *British Journal of Educational Technology*, 50(2), p. 873. Copyright 2018 by The Authors.



In the context of this study, e-assessment security is considered the degree to which authentication assurance includes presence, identity and authentication goals defined within the literature. Okada et al. (2019) found a considerable gap is to understand whether authentication systems can assure quality of the online assessment while contributing to a satisfactory assessment experience. Quality of online e-assessments includes continuously authenticated presence with the existing identity and authentication security goals (Apampa et al., 2010; Sabbah, 2017). Although quality of the security of an e-exam is important, implementation of authentication checks should not influence students' attitudes or intentions to use the system. An ideal best-practice solution for trust in e-assessment authentication should place the student in the center of the exam experience while ensuring that the system is easy to use, does not fail or is compromised during the authentication process. The system should also not affect performance and data should be kept private as outlined (Okada et al, 2019). This study aims to examine whether students trust that the continuous authentication process does not affect their privacy, exam performance, or their efforts to use the exam software. A framework for understanding student attitudes and intentions to use the system will theorize whether students believe that the continuous authentication process used during an e-assessment will affect their expectations for performance on the exam, their expectations for effort in using the exam software and their privacy concerns. This includes ensuring that the system is easy to use and there is a free effort when authenticating.

#### *Utilization and Effort Concerns*

Levy et al. (2011) warns that there is a "limited amount of research on multibiometric focused on the end user" (p. 105). Research found that "one of the most frequent concerns from students who are not satisfied with the assessment is technical problems faced when authenticating" (Okada et al., 2019, p. 870). Participants revealed that technical problems led

to exam interruptions, however it was not clearly stated if authentication methods caused the technical issues. “One of the most frequent concerns among young students who were not satisfied with the assessment refers to technical problems experienced” (Okada et al., 2019, p. 870). Levy et al. (2011) compared student intentions to use university versus vendor multi-biometric authentication during online exams and found that students are less willing to provide their biometric data to outside vendors and students raise concerns about their personal information and data being collected, archived, and used by vendors. The authors agree that investigations in the use of robust authentication approaches during online exams are highly warranted, and future work should further understand privacy and implementation concerns of vendor based multi-biometric authentication. Subsequently, privacy issues should further be explored.

### *Privacy Concerns*

The Family Educational Rights and Privacy Act (FERPA) of 1974 requires institutions to protect a student’s academic record including course name, grades, and video session of a proctored exam, however, even “the best service providers have experienced theft of data” (Brown, 2018, p. 5). Levy et al. (2011) pointed out that collecting biometric data raises student concerns regarding privacy, such as storage of personal information, biometric data, and student records, thus calling for more work to understand privacy and implementation concerns of multi-biometric data (Levy et al., 2011). Other studies found that participants have expressed concerns about data protection and privacy with the use of remote-proctoring services (Amigud et al., 2018; Bristol, 2017; Brown, 2018; Chou & Chen, 2016; Hylton et al., 2016; Miltgen et al., 2013, Lilley et al., 2016; Okada et al., 2019; Stephan, 2017). Levy et al. (2011) pointed out that third party vendors such as remote proctor may raise privacy concerns for learners. A potential concern is that “the dropout rate of e-learners may rise due to

increasing pressure to require the use of authentication approaches during e-learning course activities” (Levy et al., 2010, p. 103). Privacy has emerged as a major inhibitor of certain authentication methods (Milgen et al., 2021). Consideration should be given to whether trusted authentication levels instituted to validate the student’s identification during the e-exam would result in privacy concerns for students. In principle, it is likely that utilization concerns and privacy issues may lead students to have concerns about their exam performance.

#### *Exam Performance Concerns*

Okada et al. (2019) discovered that “participants who feel an increased level of surveillance are linked to those who feel more stressed when taking assessments due to the use of security procedures” (p. 869). Hylton et al. (2016) aimed to investigate the effects of webcam-based proctoring on misconduct during online exams, particularly how utilizing live invigilation affects a student’s test scores. Results showed that “participants not monitored had higher test scores” (Hylton et al., 2016, p. 59). The research also found a significant difference in the time that a student took to test while being proctored remotely versus not being proctored. The authors associated the difference in time to “an inclination to rush through the test due to additional anxiety resulting from the remote proctoring environment which could negatively impact test scores in comparison to participants not monitored” (p. 61). Alessio et al. (2017) found that students scored 17 points lower and used significantly less time on remotely proctored tests than on un-proctored tests. The main challenge with remote proctoring is the effort to create a balance between security, privacy, and user-friendliness (Amigud et al., 2018).

Understanding students’ trust in the authentication process includes examining privacy concerns, concerns about exam performance and concerns for utilization of the system as found by Okada et al. (2019). Further exploration will focus on an investigation of student

attitudes and intentions to use an e-assessment system that applies continuous authentication approaches to mitigate impersonation attacks. Primarily, it is beneficial to examine a student's expectations for performance on the e-assessment, their expectations for effort during the authentication process and their concerns for privacy. In addition, it may be beneficial to assess whether the level or the method of authentication applied (knowledge based, possession based or biometric based authentication) makes a difference in student effort expectancy, performance expectancy or privacy concerns. For example, a low level of authentication may have a different impact on a student's attitude and intentions to use the e-assessment system than would a higher level of authentication when applied. Moreover, the type of authentication method or combination of these methods and approaches may affect a student's trust for e-assessment in different ways. If a rigorous standard of continuous authentication is applied to ensure confidence in user security, then the system should not be compromised by impersonation threats. Even so, this may affect a student's attitudes and intentions to use the system due to expectations for exam performance, the amount of effort it may take to use the system or their concern for privacy. A conceptual framework of the various constructs to be studied rooted from the literature and their relationships can be found in Figure 3. The literature implies that there is a significant relationship between authentication assurance in e-assessment security and student concerns for the e-assessment. Student apprehensions can be based on valid concerns for security and authenticating via the e-exam platforms. Addressing these concerns that prioritizes security as well as the well-being of students requires ensuring a fair and reliable e-assessment experience. Table 4 summarizes related literature in the context of research on e-assessment and authentication assurance, which is then followed by the theoretical foundation.

**Table 4***Related Literature Review Summary*

Study	Area	Purpose
Ullah et al. (2019)	Authentication	Authentication levels and types of security
Okada et al. (2019)	Authentication	E-assessment authentication and student attitudes towards
Apampa, Wills, Argles (2010)	Authentication	Authentication security in protecting e-assessments against impersonation attacks.
Sabbah (2017)	Authentication	Authentication security in protecting e-assessments against impersonation attacks.
Moini and Mandi (2009)	Authentication	Challenges of authenticating with biometric technology
Aisyah et al. (2018)	Authentication	Types and strength of authentication methods
Gathuri et al. (2014)	Authentication	Authentication challenges in online examinations
Hylton et al. (2016)	Authentication	Deterring misconduct through remote proctoring and creating secure online exams
Laamanen et al. (2021)	Authentication	Studied perceptions of students with disabilities on the TeSLA authentication system
Chou and Chen (2016)	Privacy Concerns	Privacy issues in e-learning to measure the construct of informational privacy concerns.
Lilley (2016)	Privacy Concerns	Remote proctoring and privacy concerns
Levy et al. (2010)	Privacy Concerns	E-learners intention to provide multibiometric data during exams and privacy concerns.
Stephan (2017)	Privacy Concerns	Privacy and trust issues in e-learning environments.
Naveen et al. (2018)	Usability Concerns	User friendliness and securing exams

## **Theoretical Foundation**

As this study sought to examine user attitudes and intentions towards the use of e-authentication technologies applied during e-assessments, it was assumed that the impact of the e-authentication on e-assessments may influence students to have a reasoned negative evaluation regarding their experience. Most theories within the literature on user acceptance examine user attitudes and acceptance in non-mandatory settings such as use of a system to carry out job responsibilities. This study explored attitudes and intentions to use the system within the mandatory setting, as exams are required and tied to performance and grades. It has been found that no matter how sophisticated or powerful the technology, it is important that a user has a positive attitude towards it (Cakir & Solak, 2015). Even within mandatory settings, understanding whether people accept or reject computers can be a challenging task within information systems (Davis et al., 1989). A model adopted by researchers to understand user acceptance of information technology includes the Unified Theory of Acceptance and Use of Technology Model (UTAUT).

It has been shown that UTAUT has been used as a leading scientific paradigm for investigating and understanding the acceptance of learning technology utilized by students (Granic & Marangunic, 2019). Dwivedi et al. (2017) examined the UTAUT model and found that attitude played an important role in acceptance and intentions to use systems because an individual's attitude is shaped by the extent to which the technology is easy to use (effort expectancy) and produces greater performance (performance expectancy). In addition, the UTAUT model has been found to explain the relationship between performance expectancy and effort expectancy on behavioral intentions to use the system and considers the relationship between user attitudes and intention to use a system (Venkatesh et al., 2003). Authors also

argue that integration of perceived risks will offer a better prediction of user's behavioral intentions towards using technologies (Tarhini et al., 2014). Research also reveals that trust is required in an authentication process, yet it was found that students may distrust authentication technologies (Okada et al., 2019). One major implication is that students may be likely to reject e-authentication due to privacy concerns (Okada et al., 2019). This study employed a modified version of the UTAUT model including important constructs such as performance expectancy, effort expectancy, attitudes, and intentions to use the system with integrated constructs of privacy, perceived risks, and trust.

### **Theoretical Model**

The framework is essentially borrowed from the Unified Theory of Acceptance and Use of Technology model. UTAUT research is introduced by Venkatesh et al. (2003), an integrated theoretical model that combines eight separate models, including the TAM model, to examine an individual's intentions to use the technology. The UTAUT model introduced within this study also examined attitude towards using the technology. Research employs behavioral intentions as a vital role in understanding technology usage as the dependent variable and as an important predictor of behavior (Davis et al., 1989; Venkatesh et al., 2003). The UTAUT model determined that several constructs play a significant role in usage behaviors (2003). Two important constructs include Performance Expectancy (PE) and Effort Expectancy (EE).

PE is found to be one of the strongest determinants of intentions within mandatory use settings (Venkatesh et al., 2003; Wang et al., 2009). PE relates to the degree to which technology provides advantages (or disadvantages) to individuals while performing certain activities (Escobar-Rodriguez & Carajal-Trujillo, 2014). In the context of e-learning, this

interaction involves the perception of the end-user on their improving (or declining) their performance or increasing (or decreasing) efficiency by use of e-learning technology (Abdou & Jasimuddin, 2020). Within the e-learning environment, PE also relates to personal outcome expectations, which addresses an individual's motivation and sense of accomplishment (Tan, 2013).

EE refers to “the degree of ease associated with using the system” (Venkatesh et al., 2003, p. 450), or within the context of e-learning, “the extent to which a learner believes that using the system is a free effort” (Chiu & Wang, 2008, p. 196). The EE construct is significant within the context of mandatory use settings (Venkatesh et al., 2003). Dwivedi et al. (2019) maintains that the usefulness of information technology and a user's performance expectations and ease of effort in using the system can both influence an individual's attitude which ultimately leads to intention to use the system. Generally, if students believe that e-learning systems can help them increase their performance and it is easy to use, then there is an increase in their intention to use the technology. (Tan, 2013).

Miltgen et al., (2013) found that perceived risks variables are linked to decision making which occur in specific circumstances and for authentication systems, as privacy and identity risks are considered important. The authors identified perceived risk as a major concern for any end user based on the reputation against their privacy. Further, heightened experiences of perceived risk can result in a lower intention to adopt an authentication system. In this case, the authors concluded that the higher the invasiveness of the authentication technology, such as a biometric system, the lower the intention to tolerate the technology. Finally, trust creates an environment that is conducive to technology acceptance (Miltgen et al., 2013).

Trust is an essential factor in reducing uncertainty, risk factors, and ensuring a sense of safety and plays a central role in intentions to accept a system by reducing perceived risks. In

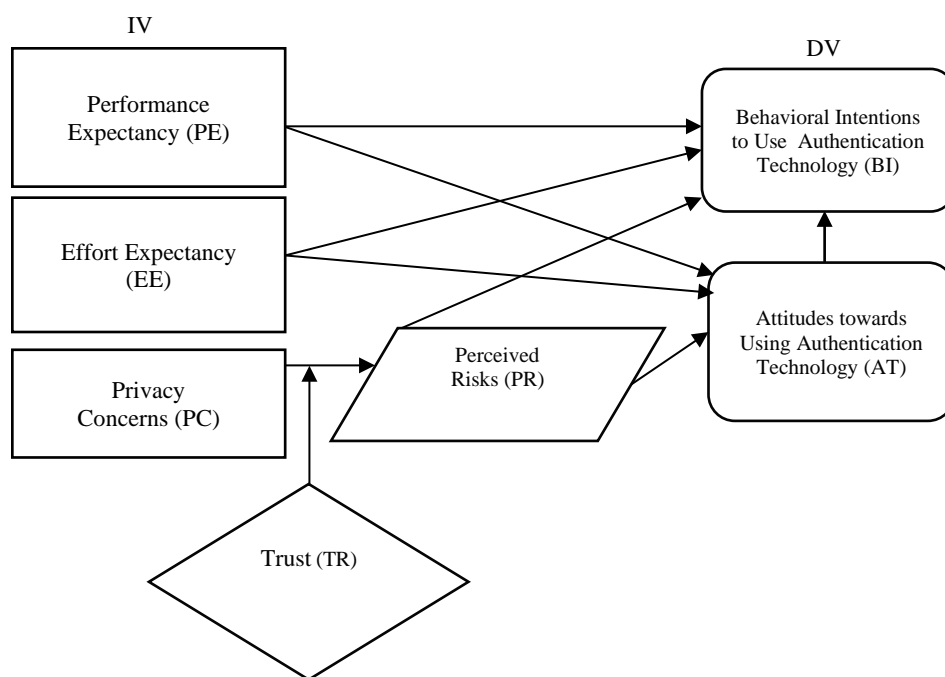


principle, as trust increases, perceived risk decreases. Trust mechanisms are present to help users cope with uncertainty including risks and a crucial element to the adoption and use of any new technology (Moriuchi, 2021). The above variables discussed have all been linked to attitudes within the literature.

Attitude has been used in several studies as a mediating variable of performance expectancy and effort expectancy (Dwivedi et al., 2019; Venkatesh et al., 2003). In addition, attitude will directly influence behavioral intention to use a system (Dwivedi et al., 2019; Rahman et al., 2017). Within this study, both intentions to use the exam system while authenticating, as well as attitude towards using the system, will function as dependent variables as advised by Chiu & Wang (2008). In addition, research by McCole et al. (2010) has found that there is a distinctive relationship between trust, attitude, and intentions to use online systems due to privacy and security concerns, as trust influences the attitudes and actions taken by users during online transactions. In summary, the following model seeks to define and connect the constructs that will be examined within this research.

**Figure 3**

*Research Model*



## **Constructs Review**

### *UTAUT Model*

According to (Khalilzadeh et al. 2017) the UTAUT model consists of six main constructs which seeks to understand the impact of effort expectancy (EE) performance expectancy (PE) social influence (SI) and facilitating conditions (FC) on behavioral intentions to use the system (BI). Behavioral intentions to use the system is one of the main dependent variables found within the UTAUT model. Therefore, to better understand whether students would favor a plan to use (or not use) continuous authentication methods when accessing an e-assessment, it is important to consider BI as a dependent variable.

PE should also be considered since performance on an e-assessment is tied to grades and success in the course. EE is also important because minimal effort should be used to continuously authenticate during the e-exam as students may become frustrated and lose focus of completing the e-assessment in an efficient and timely manner.

Within the UTAUT model, attitude has been found to have direct influence on behavioral intentions except within some cases where performance expectancy and effort expectancy are included in the model, then attitude would rather act as a mediating variable (Dwivedi et al., 2019; Rahman et al., 2017).

The following other constructs found within UTAUT were excluded from this research such as SI and FC because they are not considered within mandatory settings and usage (Venkatesh & Davis, 2000). The following will review the constructs borrowed from the UTAUT model that were used within this study.

### *Performance Expectancy (PE)*

Performance expectancy is important because attitudes regarding performance may influence academic achievement (Cakir & Solak, 2015). Within the context of learning

management systems, academic achievement is tied to performance. It has been hypothesized that people form intentions towards using a system based on how it will improve their performance (David et al., 1989; Venkatesh et al., 2003 ). According to Kharbat and Abu Daabes (2021), the more comfortable a student feels with their academic environment, the easier it may be to concentrate and achieve good performance. It has been found that PE is the “strongest predictor of intention and remains significant at all points of measurement in mandatory use settings” (Venkatesh et al., 2003, p. 447). Several studies have specifically hypothesized that PE directly affects a user’s intentions to use e-learning technologies (Abdou & Jasimuddin 2020; Chiu & Wang, 2008; Tan, 2013). This is because “if an end user is convinced that the technology is more efficient and productive, then they will be encouraged to adopt it” (Abdou & Jasimuddin, 2020, p. 40). In the same regard, if the user feels that the system would decrease productivity, then they may be less willing to use it. In summary, it is hypothesized that performance expectancy will have a direct positive effect on intentions to use the system (Rahman et al., 2017).

Positive attitudes and favorable beliefs regarding performance will create positive behavioral intention to use a technology (Rahman et al., 2017). Hence, the extent to which technology is useful and consistent with performance expectations will influence an individual’s attitude, leading to intention to use (Dwivedi et al., 2019). Therefore, it is assumed that PE is also related to attitudes towards using the technology.

#### *Effort Expectancy (EE)*

Effort expectancy derives from the beliefs that the system takes free mental effort to use (Alowayr, 2021). According to Venkatesh et al. (2003), EE stems from three existing models which includes perceived ease of use complexity, and ease of use. The authors also imply that EE is also significant in mandatory settings such as in e-assessment environments.

EE is significant in the adoption of e-learning technologies as students would want to use systems that are simple and easy to access (Abdou & Jasimuddin, 2020). It has been argued that “effort expectancy is a good predictor of intention to utilize e-learning technologies” (Abdou & Jasimuddin, 2020, p. 40). In summary, it is hypothesized that effort expectancy will have a positive effect on intentions to use the system (Rahman et al., 2017). It is also highlighted that attitude has been found to have a mediating variable on EE in several studies that used the UTAUT model (Dwivedi et al., 2019).

#### *Attitudes Towards Using Authentication Technology (AT)*

Attitudes towards using the system can be described as an individual’s reaction or feelings associated with their behavior while using the technology (Venkatesh et al.,-2003). In the context of e-learning systems, attitude is defined as “an individual’s positive or negative feeling about performing a targeted behavior” (Fishbein & Ajzen, 1975, p. 216). In the context of e-exams, it is found that student attitudes include concern for being monitored via webcam during the exam and “concern for the destination of recorded videos” (Kharbat & Abu Daabes, 2021). Attitude has been discovered as a mediating variable of PE and EE in studies that utilized the UTAUT theory (Dwivedi et al., 2019). Attitude has also been found to be the main mediator of predictor constructs on behavioral intentions (Davis et al., 1989). Laamanen et al., (2021) found a complex relationship between student attitudes and perceived advantages of using e-authentication systems. Dwivedi et al. (2019) found that attitude played a central role in acceptance and use of information technology and that it exerted an influence on usage behaviors. In essence, experiences in utilizing the system may lead users to conclude that the technology has a better (or worse) impact on performance anticipated, changing their expected consequences of utilization, and therefore affecting future intention to accept the technology (Goodhue, 1995). Beliefs about the consequences of use, and effect towards use, would lead an

individual to use or not to use the system (Goodhue, 1995). In the context of testing attitudes towards e-learning mechanisms, findings indicate that attitude plays a significant role in persuading student intentions to use or accept technologies within e-learning systems (Hussein, 2017). In brief, it has been found that attitude exerts a direct influence on intentions or usage behaviors, is a mediator between performance expectancy and intentions to use a technology and between effort expectancy and intentions to use a technology (Dwivedi et al., 2017).

#### *Behavioral Intentions to Use Authentication Technology (BI)*

Authentication is impractical if users deny or find it unacceptable, which deems acceptability of e-authentication an important issue to study (Laamaen et al. 2021). Attitude has been found to “affect behavioral intentions to use a particular technology” (Salloum et al., 2019, p. 510). Other research found attitude to have a significant relationship with intention to use or accept technologies, specifically within an e-learning system (Hussein, 2017). Miltgen et al. (2013) specifically tested biometric authentication within the construct of behavioral intention to accept the technology. Research employs intention as a key dependent variable to better understand and predict usage behaviors (Venkatesh et al., 2003). Therefore, behavioral intentions will be considered a dependent variable within this study. The following variables relate to attitudes and behavioral intentions to use the system based on findings in the literature.

#### *Perceived Risks (PR)*

Perceived risk (PR) focuses on concerns or fears in trying a new technology rather than on long term effects (Im et al., 2008). PR variables are linked to decision making which occur in specific circumstances and for authentication systems, privacy and identity risks are considered important (Miltgen et al., 2013). PR is a major concern for any end user based on the reputation against their privacy. Heightened perceptions of PR can result in a lower

intention to adopt an authentication system. In this case, the higher the invasiveness of the authentication technology, such as a biometric system, the lower the intention to tolerate the technology. Research found that perceived risk of using technology has a direct negative impact on perceived trust (Khalilzadeh et al., 2017). The rationale is that users may be sensitive to the issues of eavesdropping and will have a lack of trust in the security and privacy of the online environment (Tarhini et al., 2014). According to Im et al. (2008), the Perceived Risk construct was not considered in the UTAUT model, though the authors suggested that PR is a factor that was wrongly overlooked within the model. The authors point out that both PR and technology type both received inadequate attention in modeling UTAUT, though the anxiety construct within the model is similar to PR, with the exception of PR being short term concerns or fears of using. Further, PR is an important factor that was modeled as an antecedent of performance and a subconstruct of trust (2007).

#### *Trust in the Technology (TR)*

To recap, Okada et al. (2019) found trust in the authentication mechanism and accreditation to be important to user acceptance of the authentication technology. Trust creates an environment that is conducive to technology acceptance. Trust is an essential factor in reducing uncertainty, risk factors, and ensuring a sense of safety and plays a central role in intentions to use and accept a system by reducing perceived risks (Miltgen et al., 2013). Khalilzadeh et al. (2017) found that perceived trust positively and directly predicts intentions to use the technology. Trust in the technology may be perceived differently for different technologies. Within this research, trust level may differ based on the type of continuous authentication methods used. In the context of this research, trust may arise from privacy concerns. According to Miltgen et al. (2013), users with privacy concerns will perceive a system to be risky. Thus, continuous authentication technologies such as biometric systems

can have the potential to serve as a threat towards privacy and security which leads to potential privacy risks (Moriuchi, 2020).

### *Privacy Concerns (PC)*

Okada et al. (2019) found privacy concerns (PC) to be an imperative factor in acceptance of authentication approaches. “People who are concerned about threats to their privacy are willing to protect it” (Miltgen et al., 2013, p. 105). A perceived need for privacy, security and physical invasiveness are attitude factors that may influence intentions to use (James et al., 2008). Research found that if users are concerned about privacy and security both factors will influence perceived physical invasiveness which in turn affects intentions to use (James et al., 2008). Other research asserts that students have concerns for privacy, security and safety when authenticating during an e-exam (Ullah et al., 2019). Most users may feel fearful, hesitant, or uncomfortable using invasive authentication systems because they perceive them as a potential invasion of their privacy (Miltgen et al., 2013). Although this issue of privacy has emerged within the research, there is a need to examine the gap that exists between privacy research and end-user acceptance of invasive authentication systems (Miltgen et al., 2013). Research has found that user acceptance of authentication systems such as biometric technology can be found to be associated with privacy trust and perceived risk. Further investigation asserts that individuals with higher concerns for privacy perceive higher risks in sharing their personal identity, particularly across authentication technologies such as biometric systems. According to Miltgen et al. (2013), “Privacy concerns have also been shown to be associated with elevated levels of perceived risks”. It was necessary to borrow from existing research in order to develop constructs that could connect the relationships between the variables in this study. The following table will review background research for the constructs found within this research.

**Table 5***Constructs in Research with Associated References*

<b>Construct</b>	<b>Definition</b>	<b>References</b>
(UTAUT)- User Acceptance and Behavioral Intentions to accept	Looks at literature on acceptance through eight integrated models. Presented the constructs of Effort Expectancy and Performance Expectancy as a prediction of intention and acceptance behavior.	Venkatesh et al. (2003)
UTAUT- External Factors: Privacy, Perceived Risk and Trust	<p>The study integrates variables from the UTAUT2 model and integrates perceived privacy, and trust to understand behavioral intentions to accept use websites for purchasing flights.</p> <p>Tested privacy against perceived risk in relation to behavioral intentions to accept technology. This research addresses privacy concerns as it relates to TAM.</p> <p>Found that high trust will lead to increased perceived usefulness and perceived ease of use.</p> <p>Hypothesized that high Perceived Risks would modify the relationship between perceived use and behavioral intentions to use and between Perceived ease of use and behavioral intentions.</p> <p>Theorized that trust in the technology would have a negative impact on perceived risks. Privacy concerns have a higher perceived risk. Perceived risks will lead to lesser intention to accept a biometric system.</p> <p>Hypothesized that attitude and trust are mediators between performance expectancy and effort expectancy. Found perceive risk to have a positive impact positive direct impact on intention to use.</p>	<p>Escobar-Rodriguez &amp; Carvajal-Truillo (2014)</p> <p>Miltgen et al. (2013)</p> <p>Kanak and Sogukpinar (2017)</p> <p>Im et al. (2008)</p> <p>Miltgen et al. (2013)</p> <p>Moriuchi (2020)</p>



**Table 5** (continued)*Constructs in Research with Associated References*

<b>Construct</b>	<b>Definition</b>	<b>References</b>
UTAUT- External Factors: Privacy, Perceived Risk and Trust (continued)	<p>Found perceived risk (or perceived credibility) to have a direct relationship with behavior intention.</p> <p>Finds perceived risks to have a direct negative impact on perceive trust and perceive trust to directly affect intentions to use.</p> <p>Found perceived risk to be an antecedent of technology use and acceptance. Theorized that Perceived risk can be a direct effect of behavioral intentions as an antecedent or whether it moderates the effects of perceived use and perceived ease of use.</p> <p>Found privacy to have a positive effect on trust. Found trust to be a relevant factor within computer interaction.</p>	<p>Tarhini et al. (2014)</p> <p>Khalizadeh et al. (2017)</p> <p>Im et al. (2008)</p> <p>Escobar-Carvajal &amp; Carajal-Trujillo (2014)</p>
UTAUT Model- Performance Expectancy, TAM Perceived ease of use.	<p>Developed measurement scales for perceived ease of use and connected these variables to determinants of computer usage and user acceptance.</p> <p>End-user acceptance. Finds a positive relationship between performance expectancy and behavioral intentions to use.</p> <p>Finds effort expectancy to affect online purchase intentions.</p> <p>Finds perceive use to increase intention to accept a biometric system.</p> <p>Found Performance expectancy to be the strongest predictor of behavioral intentions to use.</p>	<p>Escobar-Rodriguez &amp; Carvajal-Truillo (2014)</p> <p>Miltgen et al. (2013)</p> <p>Im et al. (2008)</p> <p>Venkatesh et al. (2003), Moriuci (2020), Abdou &amp; Jasimuddin (2020),</p> <p>Wang et al. (2009) Raaij et al. (2008), Tarhini et al. (2014),</p> <p>Hong et al. (2011), Abdou &amp; Jasimuddin (2020), Wang et al. (2009), Tan (2013), Chiu &amp; Wang (2008)</p>

**Table 5** (continued)*Constructs in Research with Associated References*

<b>Construct</b>	<b>Definition</b>	<b>References</b>
UTAUT Model- Effort Expectancy, TAM Perceived ease of use.	<p>End user acceptance. Finds a positive relationship between effort expectancy and behavioral intentions.</p> <p>Finds effort expectancy to affect online purchase intentions.</p> <p>Finds perceive ease of use to increase intention to accept a biometric system.</p>	<p>Abdou &amp; Jasimuddin (2020), Wang et al. (2009), Moriuci (2020), Venkatesh et al. (2003), Raaij et al. (2008), Tarhini et al. (2014). Hong et al. (2017), Tan (2013), Chiu &amp; Wang (2008)</p> <p>Escobar-Rodriguez &amp; Carvajal-Truillo (2014). Miltgen et al. (2013)</p>
UTAUT Model, Acceptance Model TAM Model, Attitudes	<p>Found that attitudes play a significant role in persuading students' intention to use e-learning technologies. Attitude is determined as the strongest predictor of intentions to use or accept technologies.</p> <p>Looks at why people accept or reject computer technology by identifying how attitudes are related to perceived use and perceived ease of use.</p> <p>TAM is applied to the field of learning and found perceived usefulness (or performance expectations) on attitudes towards using the system and actual use of the system.</p> <p>End user acceptance within the banking sector. Finds attitude to have a significant influence on behavioral intentions to use.</p> <p>Finds perceived use and perceive ease of use to have a direct effect on attitudes which then has a direct effect on behavioral intentions to use.</p>	<p>Goodhue and Thompson (1988)</p> <p>Davis et al. (1989)</p> <p>Granic &amp; Maragunic</p> <p>Abdou &amp; Jasimuddin (2020)</p> <p>Khalizadeh et al. (2017) Dwivedi et al. (2019).</p>

**Table 5** (continued)*Constructs in Research with Associated References*

<b>Construct</b>	<b>Definition</b>	<b>References</b>
UTAUT Model, Acceptance Model TAM Model, Attitudes (continued)	Hypothesized attitude would have a direct relationship with behavioral intent.  Found attitude as a mediating variable between performance expectancy and effort expectancy and behavioral intention and plays a central role in accepting technologies. Attitude is defined as a significant predictor of behavioral intentions. Finds that attitude partially mediates the effect of perceive use and ease of use.	Dwivedi et al. (2019).  Rahman et al. (2017)

The goal of this research emphasized how student concerns for continuous authentication methods applied to mitigate impersonation attacks may affect students' attitudes and intentions to use the technology during an e-exam. Based on research found within the literature, some important questions were considered. The literature reflects that performance expectancy, effort expectancy and privacy issues are some concerns that students may have when using continuous authentication methods. In order to investigate how student concerns affect students' attitudes and intentions in using continuous authentication during the e-assessment the following questions were posed to assist in answering the primary research question.

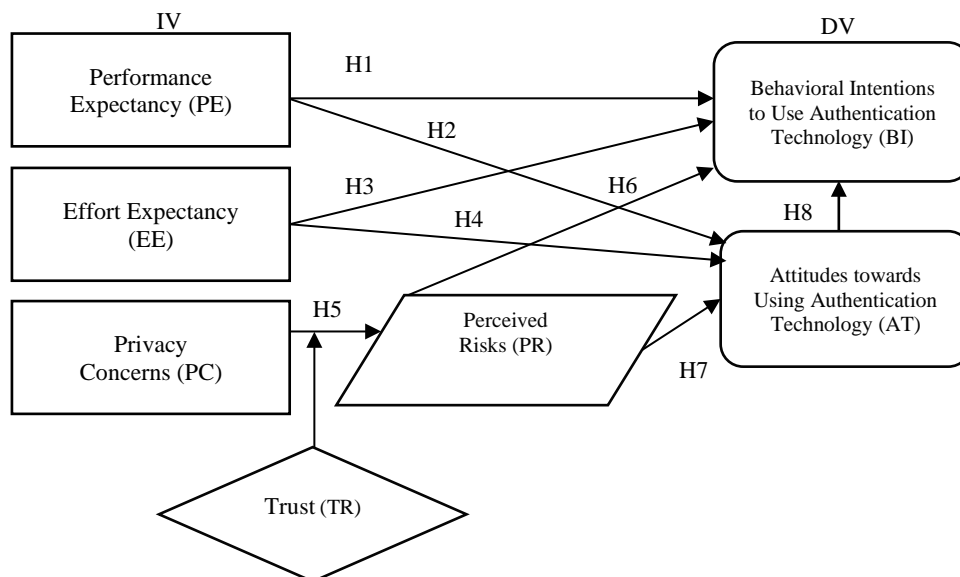
RQ1: How does performance expectancy affect students' behavioral intentions to use the continuous authentication method during an e-exam?

- RQ2: How does performance expectancy affect students' attitudes towards using the continuous authentication method during an e-exam?
- RQ3: How does effort expectancy affect students' behavioral intentions to use the continuous authentication method during an e-exam?
- RQ4: How does effort expectancy affect students' attitudes towards using the continuous authentication method during an e-exam?
- RQ5: How do privacy concerns affect students' perceived risk and how is this relationship associated with students' trust for the continuous authentication method?
- RQ6: How do privacy concerns affect students' behavioral intentions to use the continuous authentication method during an e-exam?
- RQ7: How do privacy concerns affect student attitudes towards using the continuous authentication method during an e-exam?
- RQ8: How do student attitudes towards continuous authentication methods affect their behavioral intentions to use the technology?

The relationship between the constructs discussed within this research was analyzed to understand how continuous authentication technologies may impact students' attitudes or intentions to use the e-assessment system. Essentially, the following theory is first outlined which is then followed by the hypotheses postulated for the study. The following conceptual model for this study drew upon existing literature to identify key insights and theoretical foundations, which served as a basis for formulating a hypothetical framework. Figure 4 shows the conceptual model outlined for this study which connects the relationship between each construct and the hypotheses. The model represents a synthesis of insights gleaned from the literature.

**Figure 4**

*Conceptual Research Model With Hypotheses*



*RQ1: How does Performance Expectancy affect students' behavioral intentions to use the continuous authentication method during an e-exam?* E-assessments are mandatory within online learning courses and may be a key factor as performance is tied to student grades. Which means when students expect that an e-learning website will increase their performance, they increase their intentions to use it (Tan, 2013). Davis et al. (1989) states that “people form intentions to perform behaviors towards which they have a positive affect” (p. 986). The opposite may also be true, if a technology decreases performance, users may decrease their intentions to use the technology. PE remains significant in mandatory settings and is considered the strongest predictor of intentions to use systems within this setting (Vankatesh et al., 2003). The authors identified perceive usefulness as being equivalent to performance expectations. Im et al. (2008) found strong effects of perceived use on behavioral intentions to

use a system. Alowayr (2021) found PE to be a significant predictor to use and accept mobile learning technologies and explains that when learners want to adopt an educational technology, they should feel that it will help enhance their performance outcomes. Abdou and Jasimuddin (2020) suggest that PE exhibits a considerable effect on behavioral intentions to use e-learning technologies and is based on user perception of adopting the e-technology in terms of benefits which include saving time and attaining gains of personal performance. The literature also suggests a direct relationship between performance expectancy and behavioral intentions.

***H1: PE will have a significant influence on students' BI to use the continuous authentication method during an e-exam.***

*RQ2: How does Performance Expectancy affect students' attitudes towards using the continuous authentication method during an e-exam?* Attitude may lead to a positive or negative feeling regarding the use and acceptance of e-learning technologies (Abdou & Jasimuddin, 2020). Dwivedi et al. (2019) implies that an individual's attitude towards a technology may be related to the extent to which the technology may prove useful or is associated with performance. Davis et al. (1989) linked the perceive usefulness variable to attitudes towards using the system as a user's subjective probability that using an application will increase his or her performance.

***H2: PE will have a significant influence on students' attitudes towards using the continuous authentication method during an e-exam.***

*RQ3: How does Effort Expectancy affect students' behavioral intentions to use the continuous authentication method during an e-exam?* Abdou and Jasimuddin (2020) state that EE rests on the perception of ease of use of a system. The authors claim that EE is a sound predictor of intention to utilize e-learning technologies as this construct is measured by the

user's perception in terms of benefits, such as stress-free use of the system. As an example, Wang et al. (2009) found EE to have a positive effect on BI to use mobile learning systems.

***H3: EE will have a significant influence on students' BI to use the continuous authentication method during an e-exam.***

*RQ4: How does Effort Expectancy affect students' attitudes towards using the continuous authentication method during an e-exam?* Vankatesh et al. (2003) identified perceived ease of use as being equivalent to effort expectancy. Davis et al. (1989) conducted seminal research which preliminarily found perceived ease of use to be linked to attitude towards using. Further, Salloum et al. (2019) found perceived ease of use to have a positive effect on attitude towards the use of an e-learning system. Individual acceptance of mobile learning systems can depend on whether the system is easy to use (Wang et al., 2009). Dwivedi et al. (2019) argues that "an individual's attitude can be shaped by the extent to which the technology is easy to use" (p. 728).

***H4: EE will have a significant influence on students' attitudes towards using the continuous authentication method during an e-exam.***

*RQ5: How do privacy concerns affect students' perceived risk and how is this relationship associated with students' trust for the continuous authentication method?*

Trust assists in helping people cope with uncertainty including perceived risks (Moriuchi, 2021). Im et al. (2008) refers to perceived risks as the uncertainty that affects people's confidence in their decisions. Escobar-Rodriguez and Carvajal-Trujillo (2014) state that trust is a very relevant factor in an interaction and is an essential part of a transaction and consequently users will form the intention to use a system. The authors explain that trust is associated with perceptions such as protection of their privacy. In addition, it was found that customer perception of system privacy has a positive effect on trust. Recent research has found PC or

perceived security to have an impact on TR which in turn has an impact on attitudes (Moriuchi, 2021). The authors also found PR to have an impact on TR. In this sense these constructs are significantly related. Therefore, the following hypotheses is assumed.

***H5: PC will significantly influence students to perceive the continuous authentication method as risky (PR) and TR for the technology will moderate this relationship.***

*RQ6: How do privacy concerns affect student behavioral intentions to use the continuous authentication method during an e-exam?* A study conducted by Tarhini et al. (2014) used privacy concerns to measure individuals' security, privacy and trust issues that may affect attitudes and intentions to use a system. The authors found users to be sensitive to issues of eavesdropping and found a lack of trust in the security and privacy of an online environment. Moriuchi (2021) found PR to be directly related to intentions to use the system. Van Slyke et al. (2006) concluded that PC is an important factor that affects users' willingness to use a system to conduct transactions and found that intentions to use the system were mediated by risk perceptions and trust. Escobar-Rodriguez and Carvajal-Trujillo found that trust is the strongest predictor of purchase intentions via use of online websites as the greater the trust, the more likely the intention to use the technology. Tarhini et al. (2014) ascertained that PC is one of the most influential factors that affects BI to adopt and accept a system. Zhou (2010) discovered that PC has been found to directly affect BI in a variety of contexts and insists that PC indirectly affects user behavior through TR and PR. Liu et al. (2005) found user's privacy concerns to influence their trust further determining behavioral intentions to revisit the technology. Van Slyke et al. (2006) found that PC affects intention through PR and TR. Based on the above research the following theory is hypothesized.

***H6: PC will significantly influence PR which will then influence student BI towards using the continuous authentication method during an exam.***



*RQ7: How do privacy concerns affect student attitudes towards using the continuous authentication method during an e-exam?* Miltgen et al. (2013) confirms that trust in the technology may have a negative impact on perceptions of risk specifically when accepting a biometric system. The authors also hypothesized that “the greater the perceived risk, the lesser the intention to accept a biometric system” (p. 107). Milgen et al. (2013) found that “customers with higher privacy concerns will perceive accepting a biometric system to be riskier” (p. 107). Moriuchi (2021) found perceive risk to predict attitude towards using a system and found this variable to also have “a negative impact on trust” (p. 1753). Whereas Escobar-Rodriguez and Carvajal-Trujillo found that “privacy has a positive impact on trust” (p. 76). Essentially, if a user has perceived that their privacy is secure then their trust increases, but if they have perceived risks then their trust would decrease. McCole et al. (2010) tested the relationship between PC, TR and AT and hypothesized that PC moderates the relationship between TR and AT but did not find a “non-significant moderating impact” (p. 1023). Therefore, it is hypothesized that PC will have an impact on attitudes, but this relationship is mediated by perceived risks.

***H7: PC will significantly influence PR which will then influence student attitudes towards the continuous authentication method during an exam.***

*RQ8: How do student attitudes towards continuous authentication methods affect their behavioral intentions to use the technology?*

Several studies have linked attitudes towards behavioral intentions to use. Seminal work from Davis et al. (1989) connects attitude to behavioral intentions to use a system as “BI is viewed as being jointly determined by the person’s attitude towards using the system” (p. 985). Hussein (2017) found that attitude plays a key role in students’ intentions to use e- learning technologies. Salloum et al. (2019) also proves attitude to have a positive effect on behavioral

intentions to use an e-learning system. Houssien (2017) found that “attitude plays a significant role in persuading students’ intention to use e-learning” technology (p. 163). Fishbein & Ajien (1975) also found attitude to have a positive impact on behavioral intention. Abdou and Jasimuddin (2020) found “attitude towards e-learning technology to have a considerable influence on behavioral intention to use such technology” (p. 42).

***H8: A correlational relationship exists between AT regarding continuous authentication technology and BI to use the continuous authentication technology during an exam.***

## **Summary**

Authentication methods have been used in higher education settings to mitigate impersonation attacks during e-assessments. Methods of continuous authentication may include a combination of multi-modal biometrics, invigilation, video monitoring and password verification. The OMB identified four levels of e-authentication signifying the more serious the consequence, a higher level of authentication assurance is required. In terms of impersonation attacks on e-assessments, a reliable standard would be to use a combination of authentication (or continuous authentication methods) and high levels of e-authentication assurance to mitigate impersonation attacks on e-assessments. Continuous authentication is linked to presence, identity, and authentication goals (P-I-A) and has been recommended as a method to effectively mitigate impersonation attacks. However, it is found throughout the literature that students may have concerns about privacy, utilization of the system, and expectations of poor exam performance during e-assessments. A gap found in the research is whether continuous authentication methods may affect student attitudes and intentions to use the system and whether concerns for authenticating is related to privacy issues, performance expectations, or effort expectations for using the e-exam system. Moreover, it was necessary to examine how

trust for the overall process of using the continuous authentication technology is related to student attitudes and how their attitudes may be related to their intentions to use the technology. Overall, this may vary based on the type of authentication method that is applied to mitigate impersonation attacks. Theoretical groundwork is based on the UTAUT model and was implemented to link the constructs. An online survey was devised as “it is a quicker and easier way to obtain opinions” (Miltgen et al., 2013, p. 107). The following will review methods for this research study.

## Chapter 3

### Research Methodology

#### Research Design

The general focus of this study was to design a framework for understanding the relationship between applying continuous authentication technologies on e-assessments and how this affects student attitudes and intentions to use the system. The overarching aim of this research is to explain how the identified constructs including students' performance expectations for using the exam software while authenticating, effort expectations in using the continuous authentication technology, and privacy concerns raised during the e-assessment is related to the student's intentions to use the technology, and their attitudes towards the technology. Essentially, this empirical investigation was undertaken to obtain reliable and valid data to answer the stated research question to explain the nature of the relationship between the constructs.

This research utilized the positivist approach as a paradigm to better understand the effects of implementing continuous authentication on student perceptions. "Positivist researchers hold a deterministic philosophy in which causes determine effects and outcomes" (Cresswell & Cresswell, 2018, p. 6). To understand the relationship between causes and their corresponding outcome this research looked at abstract concepts reduced into discrete variables, and then facilitated research questions to further investigate through an exploration

of the literature and subsequently hypotheses were generated to address the inquiries. A quantitative approach was then used to analyze and interpret the data.

Qualitative research explores the answer to a research problem where the variables are unknown, and the researcher needs to investigate more through exploration. Thus, the quantitative approach was the suitable approach to address the research problem since the variables were clearly defined. The main objective of using the quantitative analysis in this research was to measure and understand how performance expectancy, effort expectancy, privacy concerns, and trust for the system, is related to student attitudes and intentions to use authentication during exams. The research questions addressed within this research can best be answered through responses from research participants. In this vein, this research employed survey methods to collect data.

### **Research Method**

A quantitative approach was used to describe connections among the constructs outlined. A questionnaire was developed based on UTAUT constructs and was utilized to collect data. Attitudes are commonly measured by presenting respondents with a rating scale that covers a full range of potential evaluative responses to an object (Lavrakas, 2008). Data collection based on respondents' perceptions investigated the impact of the dependent variables; attitudes towards using and behavioral intentions to use the exam system on the independent variables Performance Expectancy, Effort Expectancy, and Privacy Concerns. It was also interesting to identify whether trust moderates the relationship between privacy concerns and perceived risk and how this relationship is related to attitudes and intentions to use the system. A survey instrument was best utilized to understand variables and to categorize, scale, code, and test for reliability and validity (Sekaran & Bougie, 2016). A Likert

5 scale delivered close-ended questions to provide a means for testing the identified items. Instructions in the questionnaire gave students a brief background of the types of authentication instruments they may have used in past online exams, the authentication levels, and types of authentication scheme for each technology. Brandon et al. (2014) recommends Qualtrics as a valuable tool to recruit research participants and distribute survey questionnaires. Therefore, Qualtrics, a web-based survey method, was utilized to facilitate the survey questionnaire. The Qualtrics survey was added to the Sona Research Participation System, an information system allowing students to participate in research at a public university. The following further addresses research method, validation, instrumentation, population, data-collection, analysis, and a method for presenting results. A summary will finalize and conclude Chapter 3.

### **Instrument Development**

A self-administered questionnaire was developed, based on prior research which has been validated and tested. According to Coughlan et al. (2009) an indebt analysis of the literature should be conducted to identify a tool that is psychometrically tested to ensure validity (measuring what the instrument is designed to measure) and reliability (that measurement is consistent). Therefore, a self-administered questionnaire was developed, based on prior research which has been previously validated and tested. The constructs of this study including (a) trust in the authentication technology (b) privacy concerns (c) effort expectancy (d) performance expectancy (e) perceived risks (f) behavioral intentions to use the system (g) and attitude towards the authentication were measured using a five-point Likert scale rating to test the abovementioned items on the instrument. Specifically, the following items were used to measure the various constructs outlined in this research. The items include suitable questions

from reliable research found within the literature that have been previously designed and tested.

*Trust in the Technology (TR)*. Items used to measure this construct will be adopted from several sources including research from Laamanen et al. (2021) who tested trust and acceptability of using e-authentication through an examination of students' attitudes. For this study, the content and validity of the data collection was tested by experts and pre-tested by students. Edwards (2018) used questionnaires aimed to ascertain participants' attitudes on trust before and after they engaged with an authentication method (TeSLA). Guerrero-Roldán et al. (2020) used a 5-point Likert scale questionnaire which ranged from strongly agree to strongly disagree, to better understand trust for authentication on e-assessment. Guerrero-Roldan et. al (2020) looks at student attitudes using several different authentication methods and authorship checking systems and students were asked several questions regarding trust in online assessment.

*Performance Expectancy (PE)*: Vankatesh (2003) used partial least squares to measure reliability and validity and used 48 separate validity tests to examine convergent and discriminant validity (p. 439). Chiu & Wang (2008) looked at intentions to use web-based learning and used factor analysis which was found significant at 0.73 or above.

*Effort Expectancy (EE)*: Several studies can be used to select items to test for effort expectancy or perceive ease of use. Cronbach alpha is 0.94 for research conducted by Moriuchi (2021) on effort expectation and intentions to use biometric technologies. Davis (1989) created effective scales for perceived ease of use with a Cronbach alpha of 0.94. Im et al. (2008) tested items on effort expectancy which had a validation of 0.94. Salloum et al. (2019) used Cronbach's Alpha to measure internal reliability of the construct items. Abou et al. (2020) also tested EE on behavioral intentions and found a Cronbach's alpha of 0.83. Im et al. (2008)

carried out a study on perceived risks and intentions to use and accept technologies and found a Cronbach's alpha of above 0.7.

*Privacy Concern (PC)*: Items will measure student concerns for privacy using research executed by Miltgen et al. (2013). The authors tested privacy concerns against perceived risks to determine behavioral intentions to use and documented a Cronbach's alpha of 0.95 and reliability of 0.96. Kharbat and Abu Daabes (2021) calculated the data on privacy concerns with a Cronbach's alpha which was 0.8 and considered satisfactory with a good level of internal consistency.

*Perceived Risks (PR)*: Im et al. (2008) tested this construct and found a reliability for the adapted items had a Cronbach alpha of 0.90. Adapted items were borrowed for this research from a study conducted by Moriuchi (2021) which had a Cronbach alpha of 0.79. Miltgen et al. (2013) tested PR on BI and found a Cronbach alpha of 0.95 and a reliability rating of 0.96.

*Trust (TR)*: Miltgen et al. (2013) found that trust has a negative impact on perceptions of risk and a positive impact on intentions. The authors reveal a Cronbach alpha 0.90 and a reliability of 0.95.

*Attitudes Towards Using (AT)*: Moriuchi (2021) utilized Cronbach's Alpha to test reliability against items which yielded a 0.94. Salloum et al. (2019) found reliability on this construct to be measured at 0.873. Guerrero-Roldán et al. (2020) used a 5-point Likert-scale and SPSS as a statistical tool to conduct data analysis on attitudes. Salloum et al. (2019) looks at the relationship between attitudes and behavioral intentions to use a system and found a Cronbach alpha of 0.8.

*Behavioral Intentions (BI)*: Technology acceptance research stems from behavioral intentions. Foundation research, such as research by Salloum et al. (2019) found Cronbach's



Alpha reliability test for items measured at 0.86. In measuring items for the intentions to use construct, Moriuchi (2021) found a 0.98 Cronbach's Alpha reliability.

Table 6 shows a list of items that were utilized to measure each construct which are listed with a description of the item and the originated source. These items were altered slightly to fit this research.

**Table 6**

*Construct Items with Associated Instrument Source*

<b>Construct/ Items</b>	<b>Description</b>	<b>Source</b>
<b>Trust in the Technology</b>	<b>Please indicate the degree to which you agree or disagree with the following statements.</b>	
TR1	The e-authentication might not work properly during an e-exam.	Laamanen et al. (2021)
TR2	The e-exam system might say I am cheating when I am not cheating	Laamanen et al. (2021)
TR3	The e-authentication might make the assessment take more time.	Laamanen et al. (2021)
TR4	It might be difficult to challenge the outcomes of e-authentication if the system questions my identity.	Laamanen et al. (2021)
TR5	Using the e-authentication system increased my trust in my e-assessment.	Guerrero-Roldán et al. (2020)
TR6	Using the e-authentication system took too much extra time.	Guerrero-Roldán et al. (2020)
TR7	The e-authentication can be intrusive.	Guerrero-Roldán et al. (2020)
TR8	The use of e-authentication for online assessment will help me trust the outcomes of my online assessment.	Edwards et al. (2018)

**Table 6** (continued)*Construct Items with Associated Instrument Source*

<b>Construct/ Items</b>	<b>Description</b>	<b>Source</b>
<b>Trust in the Technology</b>	<b>Please indicate the degree to which you agree or disagree with the following statements.</b>	
TR9	I would fully trust authenticating (with proctoring) through an e-assessment system.	Edwards et al. (2018)
TR10	I trust that using the authentication method will be careful with my personal data.	Moriuchi (2021)
TR11	I trust that my personal information will not be released to third parties	Miltgen et al. (2013)
TR12	I believe that authentication method is trustworthy	Escobar-Rodriguez & Carajal-Truillo (2014)
TR13	I trust the e-authentication and e-exam system	Miltgen et al. (2013)
<b>Privacy Concerns</b>	<b>Please indicate the degree to which you agree or disagree with the following statements.</b>	
PC1	I am concerned that my data is shared with third parties without my agreement.	Miltgen et al. (2013).
PC2	To authenticate my authorship, I have to share my personal data.	Laamanen et al. (2021)
PC3	Using the authentication system during an e-exam makes me feel nervous about being monitored.	Kharbat and Abu Daabes (2021).
PC4	I feel that opening the authentication method during online exams is impractical and would breach my privacy.	Kharbat and Abu Daabes (2021).
PC5	The concern of using an e-authentication tool for me was privacy	Kharbat and Abu Daabes (2021).
PC6	I have some concerns regarding recorded videos and pictures of me during my exams.	Kharbat and Abu Daabes (2021).

**Table 6** (continued)*Construct Items with Associated Instrument Source*

<b>Construct/ Items</b>	<b>Description</b>	<b>Source</b>
PC7	I feel like the e-authentication tools are invading my personal life and reducing my learning satisfaction.	Kharbat and Abu Daabes (2021).
PC8	I am concerned about the privacy of my personal information while authenticating during the e-exam process.	Escobar-Rodriguez & Carajal-Truillo (2014)
PC9	I trust that using the authentication method will be careful with my personal data.	Moriuchi (2021)
PC10	I trust that my personal information will not be released to third parties	Miltgen et al. (2013)
<b>Performance Expectancy</b>	<b>Please indicate the degree to which you agree or disagree with the following statements.</b>	
PE1	Using the authentication system will reduce my effectiveness on the e-exam.	Vankatesh (2003)
PE2	Using the authentication system would enable me to accomplish the e-exam task more quickly.	Vankatesh (2003)
PE3	Using the system would reduce my e-exam performance.	Vankatesh (2003)
PE4	I lose time using the authentication method when taking an e-assessment.	Olivera et al. (2014)
PE5	The authentication method would decrease my productivity during the e-exam	Im et al. (2008)
PE6	The authentication method would decrease my performance in the e-exam activity	Im et al. (2008)
PE7	Using the authentication method would diminish my effectiveness on the e-exam activity	Chiu & Wang (2008)

**Table 6** (continued)*Construct Items with Associated Instrument Source*

<b>Construct/ Items</b>	<b>Description</b>	<b>Source</b>
<b>Effort Expectancy</b>	<b>Please indicate the degree to which you agree or disagree with the following statements.</b>	
EE1	Interacting with the authentication system is often frustrating when taking an e-exam.	Moriuchi (2021)
EE2	When taking an e-exam, I believe that it is easy to use the authentication method.	Moriuchi (2021)
EE3	I often become confused when I use the authentication system when taking an e-exam.	Davis (1989)
EE4	The authentication system is rigid and inflexible to interact with.	Davis (1989)
EE5	When taking an e-exam, I believe that it is easy to use the authentication method.	Moriuchi (2021)
EE6	There is clarity and understanding in my interaction with the e-authentication technology.	Salloum et al. (2019)
EE7	The e-authentication system is easy to use for me.	Salloum et al. (2019)
EE8	Interacting with the e-authentication system does not require a lot of my mental effort.	Salloum et al. (2019)
EE9	Learning to operate the e-authentication system would be easy for me.	Im et al. (2008)
EE10	My interaction with the e-authentication technology would be clear and understandable.	Im et al. (2008), Abdou & Jasimuddin (2020), Escobar- Escobar-Rodriguez & Carajal-Truillo (2014)

**Table 6** (continued)*Construct Items with Associated Instrument Source*

<b>Construct/ Items</b>	<b>Description</b>	<b>Source</b>
EE11	The e-authentication system is easy to use.	Guerrero-Roldán et al. (2020)
EE12	When taking an e-exam, it is probable that authenticating would frustrate me because of its poor performance.	Im et al. (2008)
<b>Perceived Risks</b>	<b>Please indicate the degree to which you agree or disagree with the following statements.</b>	
PR1	I am worried about the use of the e-authentication method because people might have access to my data.	Moriuchi (2021)
PR2	The likelihood that something wrong will happen with authentication while using the e-exam system is high.	Moriuchi (2021)
PR3	Compared to other technologies, using the authentication method would have more uncertainties.	Im et al. (2008)
PR4	I feel apprehensive or uncomfortable about using the authentication method to accomplish my e-exam task	Chiu & Wang (2008)
<b>Attitude towards Using</b>	<b>Please indicate the degree to which you agree or disagree with the following statements.</b>	
AT1	I am satisfied with my experience of the e-authentication system.	Guerrero-Roldán et al. (2020)
AT2	When I use the e-authentication system, I feel an increased level of surveillance than I usually experience when taking an e-assessment.	Guerrero-Roldán et al. (2020)
AT3	When I use the e-assessment system I felt more stressed than I usually do when taking an e-assessment.	Guerrero-Roldán et al. (2020)

**Table 6** (continued)*Construct Items with Associated Instrument Source*

<b>Construct/ Items</b>	<b>Description</b>	<b>Source</b>
AT4	I think using the e-authentication tool as an authentication method is not at all effective.	Moriuchi (2021)
AT5	I think using the e-authentication tool as an authentication method is not at all valuable.	Moriuchi (2021)
AT6	I think using the e-authentication tool as an authentication method is bad.	Moriuchi (2021)
AT7	I think using the e-authentication tool as an authentication method is not at all credible.	Moriuchi (2021)
AT8	Overall, I like using the authentication method when taking an e-exam.	Salloum et al. (2019)
<b>Behavioral Intentions to Accept or Use</b>	<b>Please indicate the degree to which you agree or disagree with the following statements.</b>	
BI1	I think I am willing to try out the authentication method when taking an e-exam.	Moriuchi (2021)
BI2	I will give out my recommendation to others to use the authentication method after an e-exam.	Salloum et al. (2019)
BI3	I would like to use the authentication method on a regular basis in the future.	Salloum et al. (2019)
BI4	I will <i>not</i> recommend to other students to use the authentication method.	Alowayr (2021)
BI5	I think authentication should be implemented in e-exams	Giannakos and Vlamos (2013)

## **Validity and Reliability**

This study centers around the nature of the relationship between constructs. Construct and content validity is significant within the accuracy of research findings and speaks to how well results fit the concepts outlined in this research. Content validity asks the question of whether the instrumentation or questioner items could be efficiently utilized to measure the content of the constructs outlined within a research study (Straub et al., 2004). For example, the survey instrument (outlined in Table 6) should measure the content which it is intended to measure (Cresswell & Cresswell, 2018). To establish content validity, the survey instrument utilized in this research has undergone prior validation through an array of studies extracted from the existing literature. Further, three subject matter experts within the IS field reviewed the items on the instrument to confirm that they are relevant and representative of the construct that they are designed to measure.

Construct validity confirms that the instrument is also measuring the theories as conceptualized (Sekaran & Bougie, 2016). Straub et al. (2004) asserts that construct validity requires that measures discriminate among constructs (discriminant validity) and should be strongly associated (convergent validity). Researchers also establish construct validity by investigating correlations between measures of a construct and other measures that should theoretically be related to the construct or should vary independently from it (Westen & Rosenthal, 2003). Sekaran & Bougie (2016) also highlights correlational analysis and factor analysis as methods for establishing convergent and discriminant validity. This study utilized SPSS to validate discriminant and convergent validity by measuring patterns through correlational analysis. According to Cresswell and Cresswell (2018), some threats to internal validity include participant selection and dropout. To circumvent this, participants were required to complete the questionnaire online within one setting. In addition, generalizability is

a threat to external validity (Cresswell & Cresswell, 2018). In the case of this study, the sample was chosen from what is considered one of the largest 10 universities in the nation, therefore, the study can be generalized to other settings of similar size.

Reliability refers to ensuring consistency and stability of the instrument used for the study. It is necessary to assess whether the instrument is consistent or can be repeated and most importantly, if there is internal consistency or whether the items on the scale are intercorrelated (Cresswell & Cresswell, 2018). Cronbach's Alpha coefficient is the most used internal consistency measure and the most appropriate method to measure reliability when using Likert scales (Taherdoost, 2016). Cronbach's Alpha assumes that all items are identically scored for each construct on the scale (Straub et al., 2004). Cronbach's Alpha should pass the 0.80 standard to be considered highly reliable (Straub, 1989). However, other research cites a standard of 0.70 for confirmatory research and 0.60 for exploratory research (Straub et al., 2004). In this study, SPSS was utilized to calculate Cronbach's Alpha to demonstrate internal consistency and reliability.

### **Population and Sampling**

Survey research can provide quantitative or numeric description attitudes or opinions of a population by studying a sample of said population (Cresswell & Cresswell, 2018, p. 12). This study utilized judgment sampling, which involves the convenience of recruiting participants who are readily available to participate in the study and who can provide the information required for the research (Sekaran & Bougie, 2016). The population for this research included students who have enrolled in courses and who have taken online e-examinations whereby continuous authentication is used to secure the system against impersonation threats. Based on the research objective, as defined by Sekaran and Bougie



(2016), an appropriate sample size would be 150 to 200 participants for the research to be generalizable. This study successfully enrolled 764 research participants, exceeding the recommended sample size. The survey responses included demographic questions which revealed some important information about the research participants. This information can be found within chapter 4 of this research report.

### **Data Collection**

After receiving IRB approval from Both Nova Southeastern University and Florida International University, data was collected through a survey administered by Qualtrics software which included the participant letter and consent form. The questionnaire was uploaded to the Sona system whereby students can sign up for the study through a network that tracks their progress and gives access to the Qualtrics survey. Participants in the study were questioned on the various authentication schemes to better understand their perceptions through use of the survey instrument. Participants were first required to consent to participating in the study, and subsequently fill out demographic information. Further, the survey necessitated that students indicate the authentication method(s) they have previously employed to successfully access data across various authentication schemes.

The collected data was then exported from Qualtrics to IBM SPSS for prescreening. The prescreening process involved checking for accuracy, handling missing data, and addressing any outliers. It was important that after data is collected, that it is coded, keyed, and edited prior to conducting an analysis (Sekaran & Bougie, 2016). All missing data was re-coded to fit scales appropriately and to distinguish missing values from valid data points. All non-responses were assigned the same number and 10% or every 75<sup>th</sup> form of the coded questionnaires was checked for coding accuracy as suggested by Sekaran and Bougie.

Negatively worded items were appropriately edited using reversed scoring prior to analyzing the data.

### **Data Analysis**

A preliminary step required prior to conducting the data analysis includes the calculation and displaying basic descriptive statistics (Sekaran & Bougie, 2016). A large standard deviation may result in a high level of variability and may need further investigation (Sekaran & Bougie, 2016). Accordingly, the first step of data analysis for this research was to run descriptive statistics in SPSS to gain a comprehensive understanding of the dataset and to summarize key characteristics. The main goal of examining the descriptive statistics was to explore the frequency, distribution, central tendency, and validity of the variables. The descriptive measures allowed for a better preview of the data set to identify and understand participant characteristics, and the shape, pattern, trends, and possible outliers in the data. Other measures, as followed, were taken to ensure reliability, validity and assumptions were met prior to analyzing the data.

Once the data was checked for consistency, a Multivariate Analysis of Variance (MANOVA) was conducted to examine the effects of independent variables (PE, EE, PC) and the dependent variables (BI, AT). According to Sekaran and Bougie (2016), a MANOVA can be used to test the hypotheses to measure the mean differences among groups across the two dependent variables while controlling for the interrelationships among them. This method of statistical testing is used to quantify strength between variables and is specifically utilized when there are two or more dependent variables (Warne, 2014). A MANOVA can be used to assess main effects of the independent variables, interactions among the independent variables, and the importance of the dependent variables (French et al., 2008). MANOVA, being a

comprehensive linear model approach, is complicated in nature, nevertheless, it can demonstrate relatively lower susceptibility to type I error as compared to an ANOVA (Warne, 2014). Although a MANOVA allows for analyzing the relationship between multiple dependent variables while taking into consideration their interrelatedness, a Multivariate Analysis of Covariance (MANCOVA) allows for improved statistical power. This method is a statistical technique used to examine the relationship between a linear combination of numeric dependent variables and a set of categorical independent variables, while controlling for the effects of covariates (Vallejo et al., 2023). For a MANCOVA to provide a valid test several assumptions are required (French et al., 2008; Vallejo et al., 2023). Both MANOVA and MANCOVA were used as approaches to test the hypotheses in this research study. The two solutions suggested could both effectively be used for testing hypotheses if the data conforms to normality (Vallejo et al., 2023). Finally, macro models in statistical analysis are used for moderated mediation analysis. Hayes Process Macro model 7 is a regression-based approach which is utilized in many scholarly works. This approach was essential in examining the mediated or moderated relationships found within this research.

### **Format for Presenting Results**

An overview of the purpose of the results proceeds in study in order to outline the objectives for this research. Next, the research questions are revisited to further explain how the data was analyzed to address each research question. Descriptive statistics follow to address the sample characteristics as well as information about the relationships between the variables under study. Subsequently, verification of validity and reliability will follow. Further, research findings are unveiled. The summary of results section will address the

hypotheses in this research. Conclusions further address the research questions and explain how findings will be valuable for the practice of Information Systems as well as serve as a critical asset to higher education institutions.

### **Resource Requirements**

To complete the data collection, establish validity, and execute data analysis the following resources were utilized and were essential to the objectives of this study. The Sona system was used to ensure participant recruitment for this study and an email system was utilized to promote the study. Participants accessed the survey through the Sona system by logging in to retrieve the survey link. Qualtrics was employed to distribute and administer the survey. SPSS was utilized to convert the data, check for validity and reliability and to run descriptive and inferential statistical analysis to obtain results. Additionally, the hardware used in this research included a computer. The faculty at the university were also a resource as they assisted in promoting the study within their assigned courses. Furthermore, an expert panel was also used to approve or suggest modifications to the survey instrument. Both the Alvin Sherman Library at Nova Southeastern University and the FIU Green Library were useful in collecting the information necessary for this research. Biometric testing, hardware and software equipment was also essential but unavailable, as the biometric testing authentication hardware system needed a third-party approval but was not authorized for this research study.

### **Summary**

The research theorizes that students have genuine concerns regarding authentication methods applied to e-assessments to mitigate systems against impersonation attacks.

Specifically, trust in the authentication technology as well as privacy concerns have been pointed out as issues. Students also express concerns about expecting poor performance on the exam due to authentication issues as well as issues with their effort in using the authentication technology. This research investigates student attitudes towards authentication technologies and their intentions to use or accept an e-assessment. Descriptive and Inferential statistics are used to link the relationship between the independent and dependent variables to determine if the variables are related. Quantitative research is used to empirically investigate the questions in this study.

## **Chapter 4**

### **Results**

#### **Overview**

The main objective of this research is to answer the question of how student concerns for continuous authentication affect students' attitudes and intentions to use the technology during an e-exam. An overview of the sample population will follow which will provide information on the characteristics of research participants and the sample size. Subsequently, pre-analysis and data screening will address how reliability and validity was established prior to conducting the analysis. The data analysis section covers detailed information on the data used, and the results of statistical evaluation conducted to test the hypotheses. The results section presents the findings of the study and provides a description of what was discovered.

#### **Sample Demographics**

The sample for this research consisted of 79 (10%) male and 663 (86%) female participants ( $n=764$ ) who responded to the survey. FIU is a university based in Miami Florida and the university is diverse in nature, with a majority of Hispanic students. The data provided information on racial identity revealing that 515 individuals identified as Hispanic (86%), 100 individuals identified as black or African decent (13%), while 88 individuals identified as White/non-Hispanic (11.5%), and 20 individuals fell into the other category (3%). Most of the

respondents were psychology majors of differing academic levels as follows: Freshmen, 58 (8%) Sophomores, 99 (13%), Juniors, 370 (49%), Seniors, 207 (27%), and 8 (1%) Graduate Students, and 10 (1%) were listed as "other". Table 7 reflects the number of participants who answered the survey based on the type of authentication technology they have been exposed to during an e-exam. There were not enough participants who were exposed to biometric face recognition technology ( $N=80$ ), and biometric fingerprint verifier ( $N=12$ ). Therefore, these technologies were omitted from the study. However, The following technologies had an ample sample size and were included in the study: web-cam monitoring ( $N=471$ ), proctoring ( $N=597$ ) and lock-down browser ( $N=730$ ).

**Table 7***Baseline Characteristics of Participants*

Characteristics	WCM		PROC		LDB		Full Sample	
	<i>n</i>	%	<i>n</i>	%	<i>n</i>	%	<i>n</i>	%
Gender								
Female	408	87.20%	527	88.70%	643	88.40%	663	86%
Male	52	11.10%	57	9.60%	73	10.00%	79	10.30%
Other	8	1.70%	10	1.60%	11	1.50%	11	1.50%
Total	468	61.30%	594	77.70%	727	95.20%	764	100%
Class Standing								
Freshman	31	6.60%	46	7.80%	54	7.40%	58	7.60%
Sophomore	59	12.60%	69	11.60%	95	13.10%	99	13%
Junior	239	51.10%	297	50.10%	357	49.10%	370	49%
Senior	130	27.80%	169	28.50%	204	28.10%	207	27%
Other	9	1.90%	7	1.20%	17	2.40%	18	2.40%
Total	468	61.30%	593	77.60%	727	95.20%	764	100%
Racial Identity								
Asian	17	3.60%	21	3.50%	28	3.90%	30	3.90%
Black/African Decent	61	13.00%	75	12.60%	95	13.10%	100	13.10%
Hispanic/Latin	311	66.50%	406	68.40%	499	68.60%	515	67.4
Indig/ Natv American	4	0.90%	3	0.50%	4	0.60%	4	0.50%
White/Non-Hisp	64	13.70%	78	13.10%	85	11.70%	88	11.50%
Other	11	2.40%	11	1.90%	16	2.20%	16	2.10%
Total	468	61.30%	594	77.70%	727	95.20%	<b>764</b>	<b>100%</b>

## **Pre-Analysis Data Screening and Validation**

The constructs for this research tested for significance included performance expectancy (PE), effort expectancy (EE) and privacy concerns (PC). The dependent variables tested were attitude (AT) and behavioral intentions (BI). In addition, trust (TR) was the moderating variable and perceived risk (PR) was the mediating variable. Prior to analyzing the data on the above variables, it was necessary to further verify the dataset's validity and reliability and to ensure that all assumptions are met as required for conducting an analysis.

### *Validity and Reliability*

The judgmental approach is a method for establishing content validity through literature reviews and subsequently an evaluation by expert panel or judges (Taherdoost, 2016). This research employed the judgmental approach whereby the survey items were extracted from the literature and sequentially three experts within IS research reviewed the survey items and gave feedback for improvement.

Cronbach's Alpha is a reliability coefficient that also indicates correlation (Sekaran & Bougie, 2016). High correlations between measures or a high Cronbach's Alpha depicts signs that measures are reliable (Straub, 1989). As per Mohamad et al. (2018) for a large sample size, .5 is an acceptable recommended measure to ensure internal consistency. Scott (1995) suggests that within information systems research a Cronbach Alpha of .5 to over .7 is an acceptable form of reliability to ensure homogeneity and that the items are measuring the same phenomenon. In light of this focus on information systems research, the threshold of .5 will be utilized as a standard for this research. Appendix G shows the results of the Cronbach's Alpha test. It is evident from results of the reliability measures in Appendix G that this requirement has been sufficiently met. Assumption testing, which ensures the accuracy of the data



### *Assumption Testing*

To provide further validation with the MANOVA and MANCOVA analysis, certain assumptions must be met. Foremost, there must be independence among observations, and when dependence is suspected. For example, if measures are taken overtime from respondents (Jungbok, 2016). This research is considered a cross-sectional study whereby data was collected in a very short duration of time.

Secondly, another assumption is that multivariate normality is required. This assumption denotes that the variables are multivariate normal. However, this assumption does not impact larger sample sizes (Jungbok, 2016). Since the sample size for this research is large, this assumption should not be violated.

Another assumption required for the analyses to provide a valid test of statistical hypotheses includes a requirement that the dependent variables should be homogeneous (Vallejo et al. 2023). As shown in Appendix E, the Box's M test of equality of co-variances matrices was used to test this standard and the requirement is that the significance level should be  $p > 0.001$ . This standard was tested by using a box's test of equality of co-variance matrices as and a Levine's test of equality of error variances as reflected in Appendix F. Test results found within the appendix reflects a preponderance of the assumptions that were completely satisfied.

It is also important that there must be linearity among all pairs of dependent variables and independent variables should not have high multicollinearity as this creates redundancy in dependent measures and decreases statistical efficacy (Jungbok, 2016). According to Sekaran & Bougie (2016), multicollinearity can be checked using the correlation matrix for the independent variables and the presence of high correlation at 0.70 and above is a sign that this issue exists. The authors suggest that if there is a high correlation above the 0.70 indicator,

then the tolerance value and the variance inflation (VIF) can be used to further check and assess this problem by ensuring that the value is not at the VIF of 0.10. Thus, a correlational analysis was executed as a preliminary check on collinearity between the independent variables (PE, EE, and PC) and the dependent variables (BI & AT) (see Appendix H). The correlational analysis conducted in the matrix shows values of  $< 0.70$  between the independent and dependent variables accordingly.

A further analysis was done to check the VIF, which can be found within Appendix D. As shown in the Appendix, the value of VIF is  $< 0.10$  for all independent variables and the dependent variables within this study. It was observed that all variables in this study are somewhat related whether at the  $p$  value of 0.05 or 0.01. However, it is important to point out that correlation does not equal to causation as these findings do not translate into a cause-effect relationship. Once validity and reliability standards were checked, the data analysis was subsequently conducted.

## **Data Analysis**

This section reviews how the stated research questions were addressed in this study through statistical analysis conducted to test the research hypotheses. The variables analyzed for this research included performance expectancy (PE), effort expectancy (EE) and privacy concerns (PC). The dependent variables tested were attitude (AT) and behavioral intentions (BI). Trust (TR) was the moderator and perceived risk (PR) was the mediator.

A MANOVA analysis was conducted in SPSS to further understand the significance of the independent variables (PE, EE) in relation to the combined and distinct impact of the dependent variables (AT and BI). The results of this analysis addressed RQ1, RQ2, RQ3 and RQ4 accordingly. The independent variables (PE, EE) were categorized into two groups:

participants with either low (below the median) or high (above the median) performance expectancy, effort expectancy concerns respectively. MANOVA output results can be found within Appendix I.

Further, a multivariate analysis of covariance (MANCOVA) was conducted to examine the relationship between the effect of the last independent variable privacy concerns (PC) and the dependent variables (BI and AT). The output data for this test can be found within Appendix J. MANCOVA is particularly useful when it is suspected that specific co-variates are influencing the relationship between the dependent and independent variables. By including covariates in the analysis, one can control for their effects and isolate their relationship between the independent and dependent variables. Trust (TR) was considered a covariate, which allowed for multivariate testing. By controlling for the effects of the TR variable, a more accurate assessment of the relationship between the independent variable (PC) and the dependent variables (AT and BI) was achieved. The PC and TR variables were categorized into two groups: participants with low privacy concerns or trust for the authentication technology (those below the median) and participants with high privacy concerns or trust (those at the median and above).

Subsequently, an analysis of moderated mediation was conducted using process macro number 7 (which can be found in Appendix K). This analysis was used to test how the independent variable (PC) influences the mediator (PR), and subsequently, how the mediator impacts the dependent variables (AT and BI) considering the moderating effect of the variable (TR). The moderated mediation model was tested using a bootstrapping confidence interval approach to assess the significance of the indirect effects at differing levels of the moderator (Hayes, 2021). Moderated mediation analyses test the conditional indirect effect of a moderating variable using regression equations (Hayes, 2021). Because this path analysis

process is not a multivariate analysis, it looks at the dependent variables separately. Therefore, both the BI and AT variables are tested individually using this method. Results of the moderated mediation analysis addressed RQ5, RQ6 and RQ7.

Finally, to answer RQ8, The relationship between attitudes towards using (AT) and behavioral intentions to use (BI) were examined using Pearson correlation analysis. In essence, the above procedures were used to analyze the data to test the relationships between the variables in this study in order to address the research questions. The following section covers the findings and results of the analysis.

## **Findings**

This section presents the inferential statistical tests which will examine and uncover patterns in the data to objectively report key findings and will be discussed based on each authentication technologies investigated. Results will be broken down and discussed by each technology in the order that they were tested. Tables will reflect the outcomes and values obtained from various multivariate tests including the MANOVA and MANCOVAS along with findings from the analysis which was conducted using Hayes Process Macro model 7. The chapter concludes with a review of the findings via a discussion of the hypothesis which is essential when addressing the questions slated within this research study.

### *Proctoring*

To assess the results of proctoring authentication (PROC), the multivariate analysis of variance (MANOVA) was conducted to examine the influence of the independent variables (IVs), high and low levels of performance expectancy (PE) and high and low levels of effort expectancy (EE) on two dependent variables (DVs), behavioral intentions (BI) to use the

proctoring system and attitudes regarding the system (AT). The following were the results. Initially, a multivariate analysis looked at the impact of the independent variable on both dependent variables and subsequently, a between-subject effects test assessed each dependent variable individually.

**Table 8**

*Proctoring Authentication Method MANOVA Results*

Variables		PROC: MANOVA Results				
<b>DV-AT/BI</b>		<i>F</i>	<i>df</i>	<i>SD</i>	<i>p</i>	<i>V/ηp<sup>2</sup></i>
IV	PE	35.27	2	557	<.001	.112
IV	EE	21.28	2	544	<.001	.073
<b>DV-AT</b>		<i>F</i>	<i>df</i>		<i>p</i>	<i>ηp<sup>2</sup></i>
IV	PE	45.44	1	558	<.001	.075
IV	EE	37.75	1	545	<.001	.065
<b>DV-BI</b>		<i>F</i>	<i>df</i>		<i>p</i>	<i>ηp<sup>2</sup></i>
IV	PE	58.91	1	558	<.001	.095
IV	EE	24.52	1	545	<.001	.043

*Note.* *p* value is based on multivariate test and test of between subject effects

As shown in Table 8, the MANOVA analysis for proctoring yielded a statistically significant difference on the combined dependent variables (AT/BI). A statistically significant MANOVA effect was obtained for both PE,  $F(2, 557) = 35.27, p < .001, \eta^2 = .112$  and EE,  $F(2, 544) = 21.28, p < .001, \eta^2 = .073$ . Table 8 also shows the output for the MANOVA analysis which includes results of a test of between subject effects which tests the dependent variables separately. In light of this output, it is evident that PE has a statistically significant effect on AT,  $F(1, 558) = 45.44, p < .001, \eta^2 = 0.75$  and BI,  $F(1, 558) = 58.91, p < .001, \eta^2 = 0.95$ . The output also shows that EE also has a statistically significant effect on both AT,  $F(1, 545) = 37.75, p < .001, \eta^2 = .065$  and BI,  $F(1, 545) = 24.52, p < .001, \eta^2 = .043$ . A MANCOVA analysis subsequently followed to test the third independent variable PC. This assessment can be found in Table 9.

**Table 9***Proctoring Authentication Method MANCOVA Results*

Variables		PROC: MANCOVA Results				
<b>DV-AT/BI</b>		<i>F</i>	<i>df</i>	<i>SD</i>	<i>p</i>	<i>V/ηp<sup>2</sup></i>
IV	PC	31.74	2	530	<.001	.107
<b>DV-AT</b>		<i>F</i>	<i>df</i>		<i>p</i>	<i>ηp<sup>2</sup></i>
IV	PC	37.18	1	531	<.001	.065
<b>DV-BI</b>		<i>F</i>	<i>df</i>		<i>p</i>	<i>ηp<sup>2</sup></i>
IV	PC	53.44	1	531	<.001	.091

*Note.* *p* value is based on multivariate test and test of between subject effects

The MANCOVA yielded a significant difference between different levels of the independent variable (PC) and the dependent variables (AT/BI), when controlling for (TR),  $F(2, 530) = 31.74$ ,  $p < .001$ ,  $\eta^2 = .107$ . A statistically significant difference was also obtained between levels of PC and the dependent variables separately, AT,  $F(1, 531) = 37.18$ ,  $p < .001$ ,  $\eta^2 = .065$  and BI,  $F(1, 531) = 53.44$ ,  $p < .001$ ,  $\eta^2 = .091$ . However, to test whether (TR) moderates the path from the independent variable (PC) through the mediator perceived risks (PR) to the dependent variables (AT and BI), a regression-based approach is necessary. Therefore, a moderated mediation analysis with process model 7 was conducted.

For the proctoring authentication method, the moderated-mediation analysis is calculated with Hayes Process Macro which tested the effects of the indirect effect of the independent variable (IV), privacy concerns (PC) and the dependent variables (DV) attitude (AT) and behavioral intentions (BI) via the mediator, perceived risk (PR) with this indirect effect being moderated by trust (TR). The Hayes Process Macro, Version 7, a regression based statistical approach, was used to test the moderated mediation effects the proctoring technology. The results of this analysis for the proctoring authentication method can be found below in Tables 10-11.

**Table 10***Proctoring Authentication Moderated Mediation Results (DV:AT)*

Variables	To Mediator (PR)					To DV (AT)				
	<i>b</i>	<i>se</i>	<i>t</i>	<i>LL</i>	<i>UL</i>	<i>b</i>	<i>se</i>	<i>t</i>	<i>LL</i>	<i>UL</i>
PC	5.00	.391	12.80	4.23	5.77	-.182	.307	-.594	-.784	.420
TR	-.746	.388	-1.92	-1.51	.016					
PC × TR	-1.29	.546	-2.36	-2.36	-.214					
PR						-.340	-0.39	-8.66	-.417	-.263
Conditional direct effect [PC to PR]										
- 1 SD (TR)	5.00	.391	12.80	4.23	5.77					
+ 1 SD (TR)	3.71	.382	9.73	2.96	4.46					
Conditional indirect effect [PC to PR to AT]										
- 1 SD (TR)						-1.70	.237		-2.18	-1.25
+ 1 SD (TR)						-1.26	.200		-1.68	-.899
Index of Moderated Mediation										
						.437	.192		.082	.826

Note. Moderated mediation analysis (Process Model 7, 95% CI).

As shown in Table 10, for the path the IV (PC) to the DV (AT), the index of moderated mediation was significant,  $b = .437$ , 95% CI [.082, .826] providing evidence of a moderated mediation. There was a significant negative conditional indirect effect for high levels of trust in the proctoring technology (+ 1 SD) of the moderator (TR)  $b = -1.26$ , 95% CI [-1.68, -.899], and a stronger significant effect for low levels of trust in the proctoring technology (- 1 SD) of the moderator (TR)  $b = -1.70$ , 95% CI [-2.18, -1.25]. The a-path from the IV (PC) to the mediator (PR) there was a significant interaction between PC and TR,  $b = -1.29$ ,  $p < 0.05$ ,  $\Delta R^2 = .007$ .

The conditional effect from PC to PR was weaker for high levels of trust in the proctoring technology (+1SD) of the moderator (TR),  $b = 3.71$ ,  $p < .001$ , and it was stronger for low levels of trust in the proctoring technology (- 1 SD) of the moderator (TR),  $b = 5.00$ ,  $p < .001$ . The b-path from PR to AT was also significant,  $b = -.340$ ,  $p < .001$ . The direct effect from PC to AT was *not* statistically significant,  $b = -1.82$ ,  $p > 0.05$ .

**Table 11***Proctoring Authentication Moderated Mediation Results (DV:BI)*

Variables	To Mediator (PR)					To DV (BI)				
	<i>b</i>	<i>se</i>	<i>t</i>	<i>LL</i>	<i>UL</i>	<i>b</i>	<i>se</i>	<i>t</i>	<i>LL</i>	<i>UL</i>
PC	5.05	.389	12.98	4.28	5.81	-.762	.427	-1.79	-1.60	.076
TR	-.716	.387	-1.85	-1.48	.044					
PC × TR	-1.34	.545	-2.46	-2.41	-.270					
PR						-.460	-0.55	-8.44	-.568	-.353
Conditional direct effect [PC to PR]										
- 1 SD (TR)	5.05	.389	12.98	4.28	5.81					
+ 1 SD (TR)	3.71	.382	9.71	2.96	4.46					
Conditional indirect effect [PC to PR to BI]										
						<i>b</i>	<i>se</i>		<i>LL</i>	<i>UL</i>
- 1 SD (TR)						-2.32	.317		-2.94	-1.72
+ 1 SD (TR)						-1.71	.282		-2.28	-1.19
Index of Moderated Mediation										
						<i>b</i>	<i>se</i>		<i>LL</i>	<i>UL</i>
						.617	.255		.125	1.13

Note. Moderated mediation analysis (Process Model 7, 95% CI).

For the path from the IV (PC) to the DV (BI), the index of moderated found in Table 11 shows that the mediation was significant,  $b=.617$ , 95% CI [.125, 1.13] providing evidence of a moderated mediation. There was a negative conditional indirect significant effect for high levels of trust in the proctoring technology (+ 1 SD) of the moderator (TR)  $b= -1.71$ , 95% CI [-2.28, -1.19], and a stronger significant effect for low levels of trust in the proctoring technology (- 1 SD) of the moderator (TR)  $b= -2.32$ , 95% CI [-2.94, -1.72].

For the a-path from the IV (PC) to the mediator (PR) there was a significant interaction between PC and the moderator (TR),  $b= 1.34$ ,  $p < 0.05$ ,  $\Delta R^2 = .007$ . The conditional effect from PC to PR was weaker for high levels of trust in the proctoring technology (+1SD) of the moderator (TR),  $b = 3.71$ ,  $p < .001$ , and it was stronger for low levels of trust in the proctoring technology (- 1 SD) of the moderator (TR),  $b = 5.05$ ,  $p < .001$ . The b-path from PR to BI was also significant,  $b= -.460$ ,  $p < .001$ . The direct effect from PC to BI was *not* significant,  $b= -.762$ ,  $p = > 0.05$ . An interpretation of the relationships between the variables in



for the proctoring technology can be found as follows. The full regression table which reflects measures significant values for the path from PC to both dependent variables (AT and BI) for the proctoring technology, can be found in Table 12.

**Table 12**

*PROC Regression results for the a-path from the IV to MED and b-path MED to DV*

DV(AT)	Variables	Model a-path			Model b-c' path		
		<i>b</i>	<i>SE</i>	<i>p</i>	<i>b</i>	<i>SE</i>	<i>p</i>
IV	PC	5.00	0.391	< .001	-	-	-
MOD	TR	-	-	-	-	-	-
IV x MOD	PC x TR	-1.29	.546	< 0.05	-	-	-
MED	PR	-	-	-	-0.340	0.039	< .001
DV (BI)	Variables	Model a-path			Model b-c' path		
		<i>b</i>	<i>SE</i>	<i>p</i>	<i>b</i>	<i>SE</i>	<i>p</i>
IV	PC	5.05	0.389	< .001	-	-	-
MOD	TR	-	-	-	-	-	-
IV x MOD	PC x TR	-1.34	0.545	< 0.05	-	-	-
MED	PR	-	-	-	-0.460	0.055	< .001

*Note.* DV (AT),  $N= 530$ . Model for the a-path  $R^2 = 0.60$ ,  $F(3, 526) = 99.98$ ,  $p < .001$ , Model for b-path and c-path  $R^2 = 0.19$ ,  $F(2, 527) = 60.13$ ,  $p < .001$ . DV (BI),  $N= 531$ . Model for the a-path  $R^2 = 0.36$ ,  $F(3, 527) = 101.35$ ,  $p < .001$ , Model for b-path and c-path  $R^2 = 0.45$ ,  $F(2, 528) = 68.14$ ,  $p < .001$ .

### *Webcam Monitoring*

To assess the results of webcam monitoring authentication (WCM), the multivariate analysis of variance (MANOVA) was conducted to examine the influence of the independent variables, high and low performance expectancy (PE) and high and low effort expectancy (EE) on two dependent variables, behavioral intentions (BI) to use the web-cam monitoring system and attitudes regarding the web-cam monitoring system (AT). The results of the MANOVA can be found within Table 13. The data was examined through a multivariate analysis looking at the effects of the independent variables on both dependent variables and subsequently, a test-between subject effects looked at both dependent variables separately.

**Table 13***Webcam Monitoring Authentication Method MANOVA Results*

Variables		WCM: MANOVA Results				
<b>DV-AT/BI</b>		<i>F</i>	<i>df</i>	<i>SD</i>	<i>p</i>	<i>V/ηp<sup>2</sup></i>
IV	PE	40.80	2	399	<.001	.170
IV	EE	9.66	2	390	<.001	.047
<b>DV-AT</b>		<i>F</i>	<i>df</i>		<i>p</i>	<i>ηp<sup>2</sup></i>
IV	PE	32.25	1	400	<.001	.075
IV	EE	19.16	1	391	<.001	.047
<b>DV-BI</b>		<i>F</i>	<i>df</i>		<i>p</i>	<i>ηp<sup>2</sup></i>
IV	PE	79.49	1	400	<.001	.166
IV	EE	7.42	1	391	<.005	.019

*Note.* *p* value is based on multivariate test and test of between subject effects

As shown in Table 13, the MANOVA analysis for web-cam monitoring yielded a statistically significant difference on the combined dependent variables (AT/BI). A statistically significant MANOVA effect was obtained for both PE,  $F(2, 399) = 40.80, p < .001, \eta^2 = .170$  and EE,  $F(2, 390) = 9.66, p < .001, \eta^2 = 0.47$ . Table 13 also shows the output for the MANOVA analysis which includes a test of between subject effects. In light of this output, it is evident that PE had a statistically significant effect on both AT,  $F(1, 400) = 32.25, p < .001, \eta^2 = 0.75$  and BI,  $F(1, 400) = 79.49, p < .001, \eta^2 = .166$ . The output also shows that EE also has a statistically significant effect on both AT,  $F(1, 391) = 19.16, p < .001, \eta^2 = 0.47$  and BI,  $F(1, 391) = 7.42, p < .001, \eta^2 = 0.19$ . A MANCOVA analysis followed to test the third independent variable PC, results can be found in Table 14.

**Table 14***Web-Cam Monitoring MANCOVA Results*

Variables		WCM: MANCOVA Results				
<b>DV-AT/BI</b>		<i>F</i>	<i>df</i>	<i>SD</i>	<i>p</i>	<i>V/ηp<sup>2</sup></i>
IV	PC	67.11	2	384	<.001	.259
<b>DV-AT</b>		<i>F</i>	<i>df</i>		<i>p</i>	<i>ηp<sup>2</sup></i>
IV	PC	23.94	1	385	<.001	.059
<b>DV-BI</b>		<i>F</i>	<i>df</i>		<i>p</i>	<i>ηp<sup>2</sup></i>
IV	PC	133.96	1	385	<.001	.258

*Note.* *p* value is based on multivariate test and test of between subject effects

The MANCOVA yielded a significant difference between levels of the independent variable (PC) and the dependent variables (AT/BI), when controlling for (TR),  $F(2, 384) = 67.11$ ,  $p < .001$ ,  $\eta^2 = .259$ . A statistically significant difference was also obtained between levels of PC and the dependent variables separately, AT,  $F(1, 385) = 23.94$ ,  $p < .001$ ,  $\eta^2 = .059$  and BI,  $F(1, 385) = 133.96$ ,  $p < .001$ ,  $\eta^2 = .258$ . However, to test whether (TR) moderates the path from the independent variable (PC) through the mediator perceived risks (PR) to the dependent variables (AT and BI), a regression-based approach is necessary. In this case a moderated mediation analysis with process model 7 was conducted.

For the Web-cam authentication method (WCM) the moderated-mediation analysis is calculated using Hayes Process Macro which tested the effects of the indirect effect of the independent variable (IV), privacy concerns (PC) and the dependent variables (DV) attitude (AT) and behavioral intentions (BI) via the mediator, perceived risk (PR) with this indirect effect being moderated by trust (TR). The result of the moderated-mediation analysis is outlined in Tables 15-16 and the findings are further explained.

**Table 15**

*Web-Cam Monitoring Authentication Moderated Mediation Results (DV:AT)*

Variables	To Mediator (PR)					To DV (AT)				
	<i>b</i>	<i>se</i>	<i>t</i>	<i>LL</i>	<i>UL</i>	<i>b</i>	<i>se</i>	<i>t</i>	<i>LL</i>	<i>UL</i>
PC	5.05	.459	10.98	4.14	5.94	.138	.391	.353	-.630	.906
TR	-.738	.444	-1.66	-1.61	.136					
PC × TR	-.074	.635	-.117	-1.32	1.17					
PR						-.337	0.49	-6.90	-.433	-.241
Conditional direct effect [PC to PR]										
- 1 SD (TR)	5.05	.459	10.98	4.14	5.95					
+ 1 SD (TR)	4.97	.438	11.34	4.11	5.83					
Conditional indirect effect [PC to PR to AT]										
- 1 SD (TR)						-1.70	.324		-2.39	-1.11
+ 1 SD (TR)						-1.67	.313		-2.32	-1.09
Index of Moderated Mediation										
						.025	.220		-.407	.461

Note. Moderated mediation analysis (Process Model 7, 95% CI).

Table 15 shows that for the path from the IV (PC) to the DV (AT), the index of moderated mediation was not significant, as there is no evidence for a moderated mediation  $b = .025$ , 95% CI [-.407, .461]. There was also no significant interaction between PC and TR either,  $b = -.074$ ,  $p = > 0.05$ ,  $\Delta R^2 = .00$ . However, for the a-path from the IV (PC) to the mediator (PR) there was a significant interaction between PC and PR,  $b = 5.05$ ,  $p < .001$ . The b-path from PR to AT was also significant,  $b = -.337$ ,  $p < .001$ . However, the direct effect from PC to AT was *not* significant,  $b = 0.138$ ,  $p = > 0.05$ . A moderated-mediation analysis was further carried out to analyze the dependent variable behavioral intentions (BI), and results are listed in Table 16.

**Table 16**

*Web-Cam Monitoring Authentication Moderated Mediation Results (DV:BI)*

Variables	To Mediator (PR)					To DV (BI)				
	<i>b</i>	<i>se</i>	<i>t</i>	<i>LL</i>	<i>UL</i>	<i>b</i>	<i>se</i>	<i>t</i>	<i>LL</i>	<i>UL</i>
PC	5.12	.451	11.35	4.23	6.00	-2.22	.485	-4.57	-3.17	-1.26
TR	-.754	.435	-1.73	-1.61	.101					
PC × TR	-.146	.623	-.234	-1.37	1.08					
PR						-.445	.061	-7.33	-.564	-.326
Conditional direct effect [PC to PR]										
- 1 SD (TR)	5.12	.451	11.35	4.23	6.00					
+ 1 SD (TR)	4.97	.429	11.58	4.13	5.82					
Conditional indirect effect [PC to PR to BI]						<i>b</i>	<i>se</i>		<i>LL</i>	<i>UL</i>
- 1 SD (TR)						-2.28	.402		-3.09	-1.52
+ 1 SD (TR)						-2.21	.442		-3.11	-1.40
Index of Moderated Mediation						<i>b</i>	<i>se</i>		<i>LL</i>	<i>UL</i>
						.065	.278		-.531	.572

*Note.* Moderated mediation analysis (Process Model 7, 95% CI).

For the path from the IV (PC) to the DV (BI), as shown in Table 16, the index of moderated mediation was not significant, as there is no evidence for a moderated mediation.  $b = .065$ , 95% CI [-.531, .572]. There was also no significant interaction between PC and TR either,  $b = -.146$ ,  $p = > 0.05$ ,  $\Delta R^2 = .00$ . However, for the a-path from the IV (PC) to the mediator (PR) there was a significant interaction between PC and PR,  $b = 5.12$ ,  $p < .001$ . The

b-path from PR to BI was also significant,  $b = -0.445$ ,  $p < .001$ . The direct effect from PC to BI was also significant,  $b = -2.22$ ,  $p < .001$ . The full regression can be found in Table 17 which reflects measures with significant values for the moderated mediation path from PC to both dependent variables (AT and BI) for the web-cam monitoring technology.

**Table 17**

*WCM Regression results for the a-path from the IV to MED and b-path MED to DV*

DV(AT)	Variables	Model a-path			Model b-c' path		
		<i>b</i>	<i>SE</i>	<i>p</i>	<i>b</i>	<i>SE</i>	<i>p</i>
IV	PC	-5.05	0.459	< .001	-	-	-
MOD	TR	-	-	-	-	-	-
IV x MOD	PC x TR	-	-	-	-	-	-
MED	PR				-0.337	0.049	< .001
DV (BI)	Variables	Model a-path			Model b-c' path		
		<i>b</i>	<i>SE</i>	<i>p</i>	<i>b</i>	<i>SE</i>	<i>p</i>
IV	PC	5.12	0.451	< .001	-2.22	0.485	< .001
MOD	TR	-	-	-	-	-	-
IV x MOD	PC x TR	-	-	-	-	-	-
MED	PR				-0.445	0.061	< .001

*Note.* DV(AT),  $N = 386$ . Model for the a-path  $R^2 = 0.40$ ,  $F(3, 382) = 85.03$ ,  $p < .001$ , Model for b-path and c-path  $R^2 = 0.16$ ,  $F(2, 383) = 36.69$ ,  $p < .001$ . DV(BI)  $N = 395$ . Model for the a-path  $R^2 = 0.41$ ,  $F(3, 391) = 89.71$ ,  $p < .001$ , Model for b-path and c-path  $R^2 = 0.33$ ,  $F(2, 392) = 96.97$ ,  $p < .001$ .

#### *Lock Down Browser*

To assess the results of webcam monitoring (LDB), the multivariate analysis of variance (MANOVA) was conducted to examine the influence of the independent variables, high and low levels performance expectancy (PE) and high and low levels of effort expectancy (EE) on two dependent variables, behavioral intentions (BI) to use the lock-down browser system and attitudes regarding the lock-down browser system (AT). The data was first assessed through a multivariate analysis which looked at the effects of the independent variables on both dependent variables. Subsequently, a test-between subject effects was examined to look at both dependent variables separately. Table 18 shows the results of the MANOVA analysis.

**Table 18***Lock-Down Browser Authentication Method MANOVA Results*

Variables		LDB: MANOVA Results				
<b>DV-AT/BI</b>		<i>F</i>	<i>df</i>	<i>SD</i>	<i>p</i>	<i>V/ηp<sup>2</sup></i>
IV	PE	50.45	2	665	<.001	.132
IV	EE	14.74	2	656	<.001	.043
<b>DV-AT</b>		<i>F</i>	<i>df</i>		<i>p</i>	<i>ηp<sup>2</sup></i>
IV	PE	37.36	1	666	<.001	.053
IV	EE	27.59	1	657	<.001	.040
<b>DV-BI</b>		<i>F</i>	<i>df</i>		<i>p</i>	<i>ηp<sup>2</sup></i>
IV	PE	99.27	1	666	<.001	.130
IV	EE	15.32	1	657	<.001	.023

*Note.* *p* value is based on multivariate test and test of between subject effects

As shown in Table 18, the MANOVA analysis for lock-down browsers yielded a statistically significant difference on the combined dependent variables (AT/BI). A statistically significant MANOVA effect was obtained for both PE,  $F(2, 665) = 50.45, p < .001, \eta^2 = .132$  and EE,  $F(2, 656) = 14.74, p < .001, \eta^2 = .043$ . Table 10 also shows the output for the MANOVA analysis which includes a test of between subject effects. The output shows that PE had a statistically significant effect on both AT,  $F(1, 666) = 37.36, p < .001, \eta^2 = .053$  and BI,  $F(1, 666) = 99.27, p < .001, \eta^2 = .130$ . The output also shows that EE also has a statistically significant effect on both AT,  $F(1, 657) = 27.59, p < .001, \eta^2 = .040$  and BI,  $F(1, 657) = 15.32, p < .001, \eta^2 = .023$ . A MANCOVA test for lock-down browser follows.

**Table 19***Lock-Down Browser Authentication Method MANCOVA Results*

Variables		LDB: MANCOVA Results				
<b>DV-AT/BI</b>		<i>F</i>	<i>df</i>	<i>SD</i>	<i>p</i>	<i>V/ηp<sup>2</sup></i>
IV	PC	54.52	2	645	<.001	.145
<b>DV-AT</b>		<i>F</i>	<i>df</i>		<i>p</i>	<i>ηp<sup>2</sup></i>
IV	PC	36.08	1	646	<.001	.053
<b>DV-BI</b>		<i>F</i>	<i>df</i>		<i>p</i>	<i>ηp<sup>2</sup></i>
IV	PC	107.77	1	646	<.001	.143

*Note.* *p* value is based on multivariate test and test of between subject effects

As shown in Table 19, the MANCOVA yielded a significant difference between levels of the independent variable (PC) and the dependent variables (AT/BI), when controlling for (TR),  $F(2, 645) = 54.52$ ,  $p < .001$ ,  $\eta^2 = .145$ . A statistically significant difference was also obtained between levels of PC and the dependent variables separately, AT,  $F(1, 646) = 36.08$ ,  $p < .001$ ,  $\eta^2 = .053$  and BI,  $F(1, 646) = 107.77$ ,  $p < .001$ ,  $\eta^2 = .143$ . However, to test whether (TR) moderates the path from the independent variable (PC) through the mediator perceived risks (PR) to the dependent variables (AT and BI), a regression-based approach is necessary. In this case a moderated mediation analysis with process model 7 was conducted. For lock-down browser authentication (LDB), the moderated-mediation analysis is calculated with Hayes Process Macro which tested the effects of the indirect effect of the independent variable (IV), privacy concerns (PC) and the dependent variables (DV) attitude (AT) and behavioral intentions (BI) via the mediator, perceived risk (PR) with this indirect effect being moderated by trust (TR). The result of this analysis is explained in in Tables 20-21 which illustrates distinct effects on both dependent variables separately.

**Table 20**

*Lock-Down Browser Authentication Moderated Mediation Results (DV:AT)*

Variables	To Mediator (PR)					To DV (AT)				
	<i>b</i>	<i>se</i>	<i>t</i>	<i>LL</i>	<i>UL</i>	<i>b</i>	<i>se</i>	<i>t</i>	<i>LL</i>	<i>UL</i>
PC	5.04	.403	12.52	4.25	5.84	.185	.293	.634	-.389	.760
TR	-1.28	.393	-3.26	-2.05	-.508					
PC × TR	.321	.547	.588	-.753	1.40					
PR						-.309	0.33	-9.24	-.375	-.243
Conditional direct effect [PC to PR]										
- 1 SD (TR)	5.04	.403	12.52	4.25	5.84					
+ 1 SD (TR)	5.37	.370	14.51	4.64	6.09					
Conditional indirect effect [PC to PR to AT]										
- 1 SD (TR)						-1.56	.220		-2.02	-1.15
+ 1 SD (TR)						-1.66	.228		-2.12	-1.22
Index of Moderated Mediation										
						<i>b</i>	<i>se</i>		<i>LL</i>	<i>UL</i>
						-.099	.170		-.440	.227

Note. Moderated mediation analysis (Process Model 7, 95% CI).

For the path from the IV (PC) to the DV (AT), shown in Table 20, the index of moderated mediation was not significant, as there is no evidence for a moderated-mediation,  $b = -.099$ , 95% CI  $[-.440, .227]$ . There was also no significant interaction between PC and TR either,  $b = .321$ ,  $p = > 0.05$ ,  $\Delta R^2 = .00$ . However, for the a-path from the IV (PC) to the mediator (PR) there was a significant interaction between PC and PR,  $b = 5.04$ ,  $p = < .001$ . The b-path from PR to AT was also significant,  $b = -.309$ ,  $p = < .001$ . However, the direct effect from PC to AT was *not* significant,  $b = .185$ ,  $p = > 0.05$ .

Table 21 shows the results of the moderated mediation using Hayes Process Macro for the lock-down browser authentication. Results of the analysis showed that there are no moderated- mediation effects. However, other findings showed significant results for the mediator effect towards the dependent variable. An important observation was that the direct relationship between the independent variable, privacy concerns (PC) and the dependent variables attitudes and behavioral intentions, (AT and BI) , exhibited varied effects on the respective outcomes.

**Table 21**

*Lock-Down Browser Authentication Moderated Mediation Results (DV:BI)*

Variables	To Mediator (PR)					To DV (BI)				
	<i>b</i>	<i>se</i>	<i>t</i>	<i>LL</i>	<i>UL</i>	<i>b</i>	<i>se</i>	<i>t</i>	<i>LL</i>	<i>UL</i>
PC	5.04	.402	12.53	4.25	5.83	-.779	.393	-1.98	-1.55	-.006
TR	-1.27	.393	-3.24	-2.04	-.501					
PC × TR	.300	.546	.550	-.772	1.37					
PR						-.539	.045	-11.95	-.627	-.450
Conditional direct effect [PC to PR]										
- 1 SD (TR)	5.04	.402	12.53	4.25	5.82					
+ 1 SD (TR)	5.34	.369	14.45	4.61	6.06					
Conditional indirect effect [PC to PR to BI]										
- 1 SD (TR)						-2.71	.330		-3.40	-2.10
+ 1 SD (TR)						-2.88	.358		-3.61	-2.23
Index of Moderated Mediation										
						<i>b</i>	<i>se</i>		<i>LL</i>	<i>UL</i>
						-0.162	.294		-0.752	.387

*Note.* Moderated mediation analysis (Process Model 7, 95% CI).



For the path from the IV (PC) to the DV (BI), the index of moderated mediation, which is reflected in Table 21, was not significant, which confirms that there is no evidence for a moderated mediation.  $b = -.162$ , 95% CI  $[-.752, .387]$ . In addition, there was also no significant interaction found between PC and TR either,  $b = .300$ ,  $p = > 0.05$ ,  $\Delta R^2 = .00$ . However, for the a-path from the IV (PC) to the mediator (PR) there was a significant interaction between PC and PR,  $b = 5.04$ ,  $p = < .001$ . The b-path from PR to BI was also significant,  $b = -.539$ ,  $p = < .001$ . The direct effect from PC to BI was also significant,  $b = -.779$ ,  $p = < 0.05$ . For the full regression table which reflects significant measures for the path from PC to both dependent variables (AT and BI) for proctoring, see Table 22.

**Table 22**

*LDB Regression results for the a-path from the IV to MED and b-path MED to DV*

DV(AT)	Variables	Model a-path			Model b-c' path		
		<i>b</i>	<i>SE</i>	<i>p</i>	<i>b</i>	<i>SE</i>	<i>p</i>
IV	PC	5.04	.403	< .001	-	-	-
MOD	TR	-1.28	.393	< 0.05			
IV x MOD	PC x TR	-	-	-			
MED	PR				-.309	.033	< .001
DV (BI)	Variables	Model a-path			Model b-c' path		
		<i>b</i>	<i>SE</i>	<i>p</i>	<i>b</i>	<i>SE</i>	<i>p</i>
IV	PC	5.04	.402	<.001	-.779	.393	< 0.05
MOD	TR	-1.27	.393	< 0.05			
IV x MOD	PC x TR	-	-	-			
MED	PR				.539	.045	< .001

*Note.* DV (AT),  $N = 646$ . Model for the a-path  $R^2 = 0.38$ ,  $F(3, 642) = 129.61$ ,  $p < .001$ , Model for b-path and c-path  $R^2 = 0.16$ ,  $F(2, 643) = 61.61$ ,  $p < .001$ . DV (BI),  $N = 648$ . Model for the a-path  $R^2 = 0.37$ ,  $F(3, 644) = 128.42$ ,  $p < .001$ , Model for b-path and c-path  $R^2 = 0.29$ ,  $F(2, 645) = 136.34$ ,  $p < .001$ .

A correlational analysis was conducted to examine the relationship between attitudes (AT) and behavioral intentions (BI). The correlation between AT and BI was  $r = 0.72$ ,  $p = < 0.01$  showing a strong positive correlation, which suggests that as attitudes increase,

behavioral intentions increase as well. Appendix H shows results of the Pearson correlation matrix. These results show that for all three authentication technologies (PROC, WCM, LDB) a positive correlation was found between AT and BI.

### Summary of Results

A one-way multivariate analysis of variance (MANOVA) was conducted to test the hypotheses in order to address H1, H2, H3 and H4. The analysis was able to determine whether multiple levels of the independent variables, high and low performance expectancy (PE) and high and low effort expectancy (EE), had an effect and the dependent variables, attitudes (AT) and behavioral intentions (BI). A statistically significant MANOVA effect was obtained. For the different types of authentication methods including proctoring (PROC), web-cam monitoring (WCM) and lock-down browsers (LDB), the test found statistically significant effects with  $p < .001$  for all technologies. Conducting a test of between subject effects revealed results for a series of one-way ANOVAs on each of the dependent variables separately, the results which are listed in Table 23, yielded statistically significant effects for PE on BI and AT and for EE on BI and AT, with  $p$  values of  $p < .001$  respectively to address H1- H4.

**Table 23**

*Hypotheses Statement of Results H<sub>1</sub>- H<sub>4</sub>.*

#	Variables		Hypotheses	PROC	WCM	LDB
	IV	DV	Results	$p$	$p$	$p$
H <sub>1</sub>	PE	BI	<i>Supported</i>	<.001	<.001	<.001
H <sub>2</sub>	PE	AT	<i>Supported</i>	<.001	<.001	<.001
H <sub>3</sub>	EE	BI	<i>Supported</i>	<.001	<.001	<.001
H <sub>4</sub>	EE	AT	<i>Supported</i>	<.001	<.001	<.001

*Note.* Hypotheses tested are based on MANOVA and ANOVA results.

H1: PE will have a significant influence on students' BI to use the continuous authentication method during an e-exam. (*Supported*)

H2: PE will have a significant influence on students' attitudes towards using the continuous authentication method during an e-exam. (*Supported*)

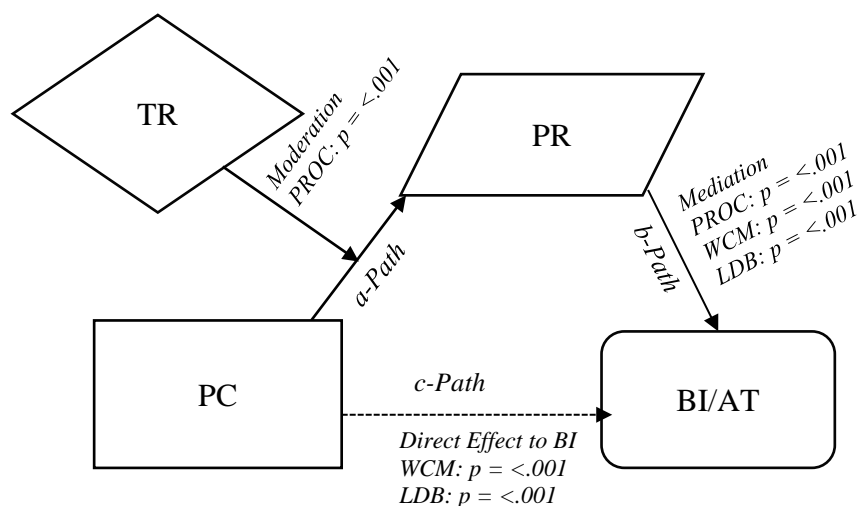
H3: EE will have a significant influence on students' BI to use the continuous authentication method during an e-exam. (*Supported*)

H4: EE will have a significant influence on students' attitudes towards using the continuous authentication method during an e-exam. (*Supported*)

A one-way MANCOVA was conducted to test the hypotheses between the independent variable, privacy concerns (PC) and the dependent variables, attitude (AT) and behavioral intentions (BI) while controlling for trust (TR) which yielded a  $p$  value of  $p < .001$  for all authentication methods. However, the moderated mediation analysis was utilized to test H5-H7 respectively. Results show the moderated mediated path analysis as outlined in Figure 5.

**Figure 5**

*Moderated Mediation Path.*



*Note.* See Appendix K for information on related output for each authentication method.

Figure 5 shows the moderated-mediation path analysis with the corresponding  $p$  values which were obtained by testing the conditional indirect effects of the moderating variable (high/low TR) on the relationship between the predictor variable (high/low PC) and an outcome variable (AT or BI) via potential mediators (PR). The analysis was utilized to measure effects of path-a, path-b and path-c respectively, for each authentication technology including proctoring (PROC) web-cam monitoring (WCM), and lock-down browsers (LDB). Table 24 summarizes these results to address H<sub>5</sub>- H<sub>7</sub>.

**Table 24**

*Hypotheses Statement of Results H5- H7.*

#	Path	Variables		PROC	WCM	LDB
		From	To	$p$	$p$	$p$
H <sub>5</sub>	<i>a-Path</i>	PC	PR	<.001	<.001	<.001
		PC × TR	PR	<0.05	* <i>n.s.</i>	* <i>n.s.</i>
H <sub>6</sub>	<i>b- Path</i>	PC	PR	<.001	<.001	<.001
		PR	BI	<.001	<.001	<.001
H <sub>7</sub>	<i>b- Path</i>	PC	PR	<.001	<.001	<.001
		PR	AT	<.001	<.001	<.001
<i>Added note**</i>	<i>a-Path</i>	TR	PR	* <i>n.s.</i>	* <i>n.s.</i>	<.001
	<i>b- Path</i>	PC	BI	* <i>n.s.</i>	<.001	<.05
	<i>b- Path</i>	PC	AT	* <i>n.s.</i>	* <i>n.s.</i>	* <i>n.s.</i>

*Note.* Hypotheses tested are based on MANCOVA and moderated mediation analysis.

\**n.s.* indicates not significant. \*\*Indicates additional results found within the analysis.

H<sub>5</sub>: PC will significantly influence students to perceive the continuous authentication method as risky (PR) and TR for the technology will moderate this relationship. (*Proc: Supported, WCM: Partially Supported, LDB: Partially Supported*) For proctoring authentication the hypotheses are fully supported. For web-cam monitoring and lock down browsers there is a significant mediation effect between privacy and perceived risks, but trust does not moderate this relationship.

H6: PC will significantly influence PR which will then influence student BI towards using the continuous authentication method during an exam. (*Supported*)

H7: PC will significantly influence PR which will then influence student attitudes towards the continuous authentication method during an exam. (*Supported*)

As outlined in Table 25, a correlational analysis was used to test the relationship between the dependent variables, attitude (AT) and behavioral intentions (BI) in order to address H<sub>8</sub> and results were found to be significant ( $p < .001$ ) for all three authentication technologies. This suggests a strong positive correlation between AT and BI. Results of the analysis show support for H<sub>8</sub>.

**Table 25**

*Hypotheses Statement of Results, Correlational Analysis to test H8.*

#	1	2
1	AT	-
2	BI	.526**

*Note.* \*\*  $p < 0.01$  level (2-tailed)

H8: A correlational relationship exists between AT regarding continuous authentication technology and BI to use the continuous authentication technology during an exam.

(*Supported*)

After an in-depth examination of the research findings in chapter 4, the overarching conclusion drawn from this research is reflected in chapter 5 to further synthesize the findings, discuss implications, and to provide recommendations for future research. The chapter serves to elicit a comprehensive understanding of what the research has uncovered and provides conclusive reflections for further solutions.

## **Chapter 5**

### **Conclusions, Implications, Recommendations, and Summary**

#### **Overview**

This chapter summarizes the main findings in this research. Conclusions are first presented, through a discussion that offers interpretations and insight and to connect and synthesize the research findings and research questions. Further, relevant literature is contextualized to relate the findings to existing literature in the Information systems field. Limitations and implications are further addressed. Finally, the chapter ends with a comprehensive summary.

#### **Conclusions**

Fundamentally, this study extrapolated constructs from the literature to examine the substantial effects of the independent variables and the relationship with the dependent variables. The variables examined gave insight to whether performance expectations, effort expectations and privacy concerns for continuous authentication technologies had any influence on student attitudes and behavioral intentions to use the continuous authentication technology during e-exams. Further, the research investigated whether trust would affect the strength of students' privacy concern for the technology and whether their perceived risks would explain the reasons for their attitudes and intentions to use the authentication technology. To uncover this inquiry, data was collected, and a multi-method analysis was conducted to gain insight to how these variables are connected.

The results of the study which was analyzed through multivariate testing provided information about the overall effect of the independent variables (performance expectancy, effort expectancy and privacy concerns) and the dependent variables (attitudes and behavioral intentions). The analysis showed statistically significant effects, suggesting that these independent variables have a significant influence and the dependent variables, which helped to answer the following research questions (*RQ1- RQ4*).

*RQ1: How does Performance Expectancy affect students' behavioral intentions to use the continuous authentication method during an e-exam?* Findings indicate that performance expectancy significantly influences students' behavioral intentions to use the continuous authentication system during e-exams.

This suggests that if students perceive the authentication system to positively impact their exam performance, then this will have an effect on their behavioral intentions. This also implies that if the students have a negative perception of how the authentication system affects their exam performance, this is likely to result in an effect on their behavioral intentions towards using the exam.

This finding is consistent with several studies that found that intentions toward using a system is based on how it will improve the user's performance (Alowayr, 2021; Cakir & Solak, 2015; David et al., 1989; Escobar-Rodriguez & Carajal-Truillo, 2014; Venkatesh et al., 2003). Within the context of e-learning technologies, other research has linked performance expectancy directly to a user's intentions (Abdou & Jasimuddin 2020; Chiu & Wang, 2008; Tan, 2013). It was hypothesized that performance expectancy will have a direct effect on intentions to use a system (Rahman et al., 2017). These findings align consistently with the findings in this study as this study found that performance expectancy significantly influences students' behavioral intentions to use the authentication system during e-exams. Vankatesh et

al. (2003) found performance expectancy to be the strongest predictor of intentions in mandatory settings. In addition, Abdou & Jasimuddin (2020) found a significant relationship between performance expectancy and behavioral intention to use e-learning technology with a significant p-value ( $p = < .001$ ). Within the framework of this investigation, participants who engaged in e-exams via an e-learning systems where authenticating was mandatory during an e-exam gave feedback on their experience. Results indicate statistically significant differences in behavioral intentions across levels of performance expectancy ( $p = < .001$ ). The overall implication, which is consistent with the literature, is that performance expectancy significantly influences behavioral intentions. The effect size of this impact is moderate to high (9.5%-16.6%) of the variability in behavioral intentions can be attributed to a student's performance expectancy. For proctoring authentication performance expectancy explained 9.5% of the variance ( $R^2$ ), for lock-down browser, an effect size of 13% was found while webcam monitoring had the higher effect size (16.6%). This finding may be an indication that performance expectancy is a meaningful contributor, although, other factors influencing behavioral intentions are also likely. Nonetheless, It may be useful to explore interventions or strategies that can influence or manage performance expectations to enhance positive behavioral intentions.

*RQ2: How does Performance Expectancy affect students' attitudes towards using the continuous authentication method during an e-exam?* Findings indicate that performance expectancy significantly influences students' attitudes to use the continuous authentication system during e-exams.

For all three continuous authentication technologies analyzed, the way that students expect to perform on an exam had a very high and significant effect on their attitudes towards using the authentication method. In this context, students who express high concerns for



performance expectancy will also shape their attitudes towards the authentication method. The analysis suggests that as individuals anticipate improved exam performance through the use of the authentication technology, their attitudes towards the technology be affected. Conversely, If individuals anticipate that the authentication technology would hinder or negatively impact their exam performance, their attitudes towards the technology could also be affected. Seemingly, students' concern for not performing well on an e-exam due to having used an authentication technology could potentially have an effect on their attitudes towards the technology.

Attitudes can lead to either a positive or negative attitude in the context of e-learning technologies (Abdou & Jasimuddin, 2020). Studies have found that attitude towards a technology to be related to how the technology is related to performance (Dwivedi et al., 2017). The authors found that the extent to which technology is useful and consistent with performance expectations will influence an individual's attitude. This research study by Dwivedi et al. ascertained highly significant results ( $p < .01$ ), which suggests that differences in users' performance expectations may impact a user's attitude towards the authentication system.

Similar to the findings in that study, this analysis also indicated a statistically significant p-value ( $p < .001$ ), with a substantial effect size which indicated that at least 5.3% - 7.5% (based on the technology) of the variability ( $R^2$ ) in attitudes can be attributed to the expectancy of enhanced exam performance. For the proctoring authentication method, performance expectancy explained 7.5% of the variance ( $R^2$ ) in attitudes towards using this continuous authentication method. For web-cam monitoring, performance expectancy explained the variance ( $R^2$ ) in attitudes by 7.5% and for lock-down browsers, by 5.3%. According to Kharbat and Abu Daabes (2021) the fewer concerns that students have about

using technologies such as e-proctored exams, the more positive impact this would have on their academic performance. Intervention strategies should be assessed to ensure that users have positive attitudes when taking an e-exam, specifically because this requirement is tied to grades.

*RQ3: How does Effort Expectancy affect students' behavioral intentions to use the continuous authentication method during an e-exam?* Findings indicate that effort expectancy significantly influences students' behavioral intentions to use the continuous authentication system during an e-exam.

For all three continuous authentication methods, there was a statistically significant influence of effort expectancy on behavioral intentions to use the authentication method during an e-exam. This implies that students' perceptions of the expected effort when using the system significantly contributes to their intentions to use the system. In summary, when students perceive the expected effort of using the authentication system, whether positively or negatively, it has a significant influence on their intentions to use the system during an exam.

Venkatesh et al. (2003) states that effort expectancy is significant in mandatory settings such as e-learning environments. Salloum et al. (2019) found that an e-learning system's ease of use has a positive effect on behavioral intentions to use the system indicated by the p-value ( $p = < 0.05$ ). Chiu and Wang (2008) also found that effort expectancy is related to intentions to continue using web-based learning systems which was indicated by the p-value ( $p = < 0.05$ ). Other studies found that effort expectancy is a good predictor of intention to use e-learning technologies (Abdou & Jasimuddin, 2020). Rahman et al. (2017) also found effort expectancy has a positive effect on intentions to use a system. Studies have found effort expectancy to be a key predictor of intentions to use e-learning technologies (Wang et al., 2009). Abdou &

Jasimuddin (2020) found a significant relationship between effort expectancy and behavioral intentions to use e-learning systems indicated by the p-value ( $p = < .001$ ).

In the context of this research analysis, significant effects were also found in relation to differences in the levels of effort expectancy perceived and how this relates to behavioral intentions towards the authentication system ( $p = < .001$ ). The effect size is somewhat small (1.9%-.4.7%) based on the technology. For proctoring, 4.3% of the variance ( $R^2$ ) in behavioral intentions is explained by effort expectancy, 1.9% for web-cam monitoring, as well as 2.3% for lock-down browsers. Although effort-expectancy explains a small percentage of the variance in behavioral intentions to authenticate during an e-exam, this finding should be taken into consideration. When implementing authentication systems during e-exams, it may be necessary to manage student's perceptions of effort in using the system to positively influence behavioral intentions.

*RQ4: How does Effort Expectancy affect students' attitudes towards using the continuous authentication method during an e-exam?* Findings indicate that effort expectancy significantly influences students' attitudes to use the continuous authentication system during an e-exam.

For all three continuous authentication methods, students' expectations about how much effort it would take to use the system seems to have significant effects on their attitudes towards using the system. The results of the analysis revealed a statistically significant impact of effort expectancy on attitudes. In this regard, students may appreciate the additional effort required to authenticate if they understand the importance of the authentication technology, leading to a higher acceptance of the technology. However, if users do not see the additional effort as justified, it may lead to negative attitudes towards the system.

Overall, studies have found that acceptance of learning systems can depend on whether it is easy to use (Wang et al., 2009). Salloum et al. (2019) found that an e-learning system's ease of use has an effect on attitudes to use the system indicated by the p-value ( $p = < 0.05$ ). Also, research found that an individual's attitude is shaped by how easy the technology is to use and that attitude tends to be a facilitator of effort expectancy (Dwivedi et al., 2019).

The outcome of this research aligns consistently with findings in the literature. There is an impact found on the levels effort expectancy and attitudes regarding continuous authentication systems which yielded a significant level ( $p = < .001$ ). The effect size ranged from 4.0% - 6.5% based on the authentication technology. For proctoring, 6.5% of the variability in attitudes can be attributed to effort expectancy. Webcam monitoring explained 4.7% and lock down browsers explained (4.0%) of the variance ( $R^2$ ) in attitudes. With the implementation of authentication systems, understanding the amount of effort users perceive may impact their attitudes may be useful in implementing strategies to improve the user experience, such as user training on authenticating prior to using the system.

*RQ5: How do privacy concerns affect students' perceived risk and how is this relationship associated with students' trust for the continuous authentication method?*

Privacy concerns contribute to lower perceived risk associated with the continuous authentication technology and privacy concerns and perceived risks are likely associated with lower trust for the proctoring authentication method.

In essence, it is apparent that higher privacy concerns are likely to influence students' perceived risk positively for all three technologies. This research found that increased privacy concerns lead to higher perceived risks for proctoring, web-cam monitoring and lock-down browsers. This finding aligns with results reported within the literature such as with research conducted by Zhou (2010), who found certain privacy concerns to be positively related to

perceived risks, at the significance level of ( $p < 0.01$ ). For all three technologies, findings indicate that one-unit increase in privacy concerns is associated with a 5 unit increase perceived risks and this relationship is positively associated. This finding is also consistent Miltgen et al. (2013), who found that customers with higher privacy concerns for biometric systems will perceive the technology as riskier. Other research by Zhou (2010) similarly rejected the hypothesis that privacy concerns affect trust for location-based technologies. In essence, findings in the literature reveal a statistically significant and positive association between privacy concerns and perceived risks. However, studies indicate diverse findings concerning the relationship between trust, privacy concerns and perceived risks based on the technology being examined. For example, studies have hypothesized that customer trust in biometric technology would have a negative impact on perceived risks, though this hypothesis was rejected (Miltgen et al., 2013). However, other research on acceptance of location-based services, by Zhou (2010), found trust to have a negative association with perceived risks and a negative association with privacy concerns. Other research found perceived risk of using a mobile based payment technology to have a direct negative impact on perceived trust (Khalilzadeh et al., 2017). Other research looking at mobile banking technology agrees that perceived risks have a negative impact on trust (Almaiah et al., 2023).

Likewise, based on the analysis conducted in this study the interaction between the moderator (trust in the proctoring technology) and the independent variable (privacy concerns) on the mediator (perceived risks) suggests that the relationship between students' experiences with the authentication technology and their trust in the proctoring system, depends on the level of trust and the type of authentication method. For students with high trust (+ 1 SD), the indirect effects on both attitudes and behavioral intentions are significant but less of an influence compared to those with low trust (-1 SD). In summary, privacy concerns influence

perceived risks, and the strength of the effect varies based on the level trust in the authentication technology. This holds true only for proctoring authentication, as a one-unit increase in the interaction between trust and privacy results in a one unit increase in perceived risks which indirectly affects behavioral intentions and attitudes more so for those with low trust rather than those with high trust.

However, for webcam monitoring and for lock-down browsers, an increase in privacy concerns is associated with an increase in perceived risks but trust does not moderate this relationship. This signifies that for students' experiences with webcam monitoring and lock-down browsers, an increase in their privacy concerns is associated with an increase in their perceived risks or confidence in using the system , but this relationship does not vary based on the different levels of trust for the continuous authentication method.

*RQ6: How do privacy concerns affect student behavioral intentions to use the continuous authentication method during an e-exam?* Findings indicate that an increase in privacy concerns is associated with an increase in perceived risks and perceived risk is negatively associated with behavioral intentions towards the authentication technology.

As pointed out, an increase in privacy concerns is associated with an increase in perceived risks. Studies have associated privacy concerns directly with perceive risks for authentication methods such as biometric technology (Miltgen et al., 2013). These findings are aligned with results found in this research which suggests that as students become more concerned about privacy, then their perceived risks or their judgement or uncertainty about the system is suggested to increase as well. Further, this relationship in turn is positively associated with behavioral intentions (intention to use the system). This implies that if students have high uncertainty about using the system or if they have increased perceived risks in it then this negatively impacts their behavioral intentions. Therefore, if students perceived risks or

uncertainty about using the technology increases then their behavioral intentions to use the system is negatively influenced. This could potentially result in a reduced intent for learners to use the system in the future. This finding is closely related to research found within the literature whereby perceived risks were found to have a negative direct relationship with intention to use facial recognition technology which was found to be statistically significant at the level of  $p < 0.05$  (Moriuchi, 2021). Miltgen et al. (2013) also found greater perceived risks to be associated with lesser intentions to accept systems (such as biometric technologies). Further, Zhou (2010) observed that perceived risks negatively affect usage intentions for location-based technologies, and this relationship was found to be significant at the p-value ( $p = 0.001$ ).

An additional related finding in this analysis, which was not in the scope of this research, is that privacy concerns had a direct impact on behavioral intentions, for the web-cam monitoring and lock-down browser technology. As students' privacy concerns increase for the authentication method, then their behavioral intentions towards the technology tend to decrease. In the same way, if privacy concerns decrease, then behavioral intentions will increase for the authentication methods. This does not hold true for the proctoring technology as privacy concerns are contingent on an increase in perceived risks which indirectly affects behavioral intentions.

*RQ7: How do privacy concerns affect student attitudes towards using the continuous authentication method during an e-exam?* An increase in privacy concerns is associated with an increase in perceived risks and an increase in perceived risk is negatively associated with attitudes towards the authentication technology. Other literature findings associate privacy concerns directly to perceive risks for authentication methods such as biometric technology (Miltgen et al., 2013). In essence, higher privacy concerns are linked to higher perceived risks.

This suggests that as students become more concerned about privacy, then their perceived risks or their judgement or uncertainty about the system is suggested to increase. Further, this relationship in turn is negatively associated with attitudes about the technology. This implies that perceived risks play a negative role in shaping students' attitudes towards the technology. If perceived risks or uncertainty increases then positive attitudes will decrease, if uncertainty decreases then positive attitudes will increase. This finding is closely related to research found within the literature whereby perceived risks were found to be statistically significant ( $p < 0.01$ ) in predicting customer attitudes towards facial recognition technology (Moriuchi, 2021). Other research found perceived risks to be negatively associated to attitudes towards mobile banking technologies (Almaiah et al., 2023).

This study found a significant positive association between privacy concerns and perceived risks across all authentication technologies examined and this relationship was statistically significant ( $p < 0.001$ ). Further, perceived risk was found to be negatively associated with attitudes at a statistically significant level ( $p < 0.001$ ) for all authentication methods. An additional finding, which is outside the scope of this study, uncovered that privacy concerns do not have a direct impact on attitudes for any of the authentication methods examined. In essence, an extension of this research revealed that privacy concerns alone would not likely affect students' attitudes about the authentication technology without the presence of perceived risks.

*RQ8: How do student attitudes towards continuous authentication methods affect their behavioral intentions to use the technology?* There is a positive correlation between attitudes and behavioral intentions to use an authentication technology.

The analysis suggested a positive relationship exists between attitudes and behavioral intentions. As attitudes become more positive, individuals are more likely to express stronger



intentions to engage in using the authentication system. However, as attitudes become more negative then individuals are likely to have weaker intentions to use the authentication system. It is important to express that this does not mean that attitudes cause behavioral intentions and conversely behavioral intentions do not cause attitudes. These findings are in line with research on acceptance for learning management systems, which suggests that attitudes positively influence behavioral intentions, and this relationship is significant ( $p < 0.001$ ), (Salloum et al., 2019).

In summary, the objective of this study was to find out whether there are significant concerns for continuous authentication methods through an analysis of the associated constructs. This analysis implied that performance expectancy, effort expectancy and perceived risks were significantly related to behavioral intentions and attitudes towards using continuous authentication during e-exams. Further, privacy concerns are positively associated with an increase in perceived risks and this relationship is moderated by levels of trust in the proctoring technology. The moderation effect was true for proctoring authentication but for web-cam monitoring and lock-down browsers, the effect between privacy concerns and perceived risks did not vary based on the different levels of trust. Additionally, it was found that an increase in perceived risks is negatively associated with both attitudes and behavioral intentions to use the authentication technology. In summary, if privacy concerns increase then perceived risks (or uncertainty) tend to increase, which in turn leads to a negative impact on attitudes and behavioral intentions. Another related finding indicated that for web-cam monitoring and lock-down browsers, privacy concerns are directly negatively associated with behavioral intentions. However, this does not hold true for proctoring, which requires perceived risks as an indirect mediator to behavioral intentions. Although a majority of the findings demonstrated significance, there were limitations to the study, which will be further addressed.

## **Limitations**

The study had some associated limitations. The research objective set out to look at several different technologies which are used to prevent impersonation attacks during e-exams, including web-cam monitoring, proctoring, lock-down browser technology and biometric technologies such as biometric fingerprinting and face recognition technologies. However, there was a barrier to obtaining data for the biometric technologies (finger-print scanner and facial recognition software) as there were a small amount of the sample population who have accessed this technology. In addition, the study was based on user perceptions, which can be influenced by personal biases, experiences or cultural backgrounds. Furthermore, the participants were students from one distinct university consisting of a unique student population which comprised of predominately females. Finally, it is noteworthy that the study's reliance on a large sample size may have contributed to the detection of statistically significant effects. However, the observed small to moderate effect sizes found sheds light on the importance of exploring alternative methodologies and diverse samples when replicating these findings to ensure practical reliability and generalizability.

## **Implications**

This research could contribute significantly to the information systems (IS) field by disseminating information that can provide knowledge to the professional practice. The findings can allow for higher education administration, instructors and instructional designers to consider the concerns of students when designing policy for required authentication while taking e-exams. The research sheds light on the user experience of students interacting with

continuous authentication technologies. Understanding how students receive and respond to these technologies contributes to discourse on user experience within the realm of information systems. The research also provides insight on security concerns and privacy concerns in order to balance security measures while taking into consideration user acceptance. By focusing on technologies designed to mitigate impersonation attacks, the study addresses an aspect of cybersecurity within information systems. As AI technologies increasingly facilitate unwarranted assistance in e-exams, there is a growing need for emerging technologies to counteract and prevent students from strategies such as impersonation schemes. This research can serve to ensure that these emerging technologies are developed with the user in mind. Most importantly, the research has implications for formulation of educational technology policies. For example, the finding that proctoring has an impact on behavioral intentions and attitudes due to perceived risks has implications for training proctors to decrease privacy concerns and decrease uncertainty to ensure that students have positive authentication experience. Understanding student concerns and expectations can help to guide development of technologies that balance security and a positive user experience. Specifically, this research contributes a method for examining technologies using a multi-method multivariate analysis to better understand how these tools can affect users. Accordingly, there may be implications for future IS research.

### **Recommendations**

Specifically, this research underscores the importance for higher education institutions to consider students' perceptions of behavioral intentions and attitudes towards authentication systems used to mitigate impersonation attacks during e-exams. The findings suggest that the way students perceive their performance on the exam, the effort it takes to authenticate during

the exam and their privacy concerns significantly influences their behavioral intentions to use the system and their attitudes towards the system. The study also finds that students' privacy concerns are significantly associated with their perceived risks for the authentication technologies examined. If privacy concerns increase, then perceived risks or uncertainties in the technology also increase which negatively impacts their attitudes and behavioral intentions to use the system. Therefore, if students perceive risks for the technology, then their behavioral intentions and attitudes will also be negatively affected. In addition, for the proctoring technology, findings indicated that privacy concerns can indirectly influence attitudes and behavioral intentions through perceived risks and this mediation is moderated by trust.

One suggestion arising from the investigation is the necessary implementation of policy. A student should gain a comprehensive understanding of the purpose and overall benefit of authenticating and the benefits of instituting these security measures that are designed to consider all parties involved.

Recommendations for future research include a further examination of the continuous authentication technologies to understand how levels of authentication are related to the constructs outlined within this research. This research suggests that proctoring has distinct outcomes as compared to web-cam monitoring and lock-down browsers. A study can take a closer look at user experience for each of the authentication methods taking into consideration the four authentication levels as well as the strength of the security applied. A closer examination may help to shed light on why the conceptual model fully explains the proctoring authentication method versus web-cam monitoring and lock-down browser technology. For instance, it was found that for proctoring trust moderates the relationship between privacy concerns and perceived risks which in turn mediates the relationship between privacy concerns and behavioral intentions as well as attitudes. Another nuance, although outside the scope of

this study, is that privacy concerns for web-cam monitoring and lock-down browsers has a direct negative effect on behavioral intentions to use the system as compared to proctoring systems which showed more of a moderated and indirect effect. A comprehensive review that connects these findings to the levels of authentication and how this is connected to perceptions of the different authentication methods would be beneficial and can be addressed through a future research study. It would also be interesting to readdress biometric face recognition and fingerprint scanning authentication technologies within the context of this research if there is an opportunity to the associated collect data. The age of the participants may also be a key to a better understanding of the population and whether their perceptions differ for these types of authentication technologies. Additionally, for a more comprehensive understanding of the student experience, future research could look at specific aspects related to student status, based on college levels, given that a predominant number of students in this study were juniors in college. Finally, other independent variables associated with authenticating during an e-examination that may affect attitudes or behavioral intentions such as anxiety during an e-exam due to required continuous authentication can also be examined.

## **Summary**

The lack of face-to-face interaction in e-learning environments motivates collusion by students during summative examinations (Ullah et al., 2016). Students were required to learn to adapt to online examinations due to the current learning environment. Student authentication is a major challenge in higher education and for institutions and within online learning, impersonation is a threat (Laamaen et al., 2021). Specifically for e-assessments, impersonation attacks are considered a major concern and are recognized as a great risk within the academic community (Apampa et al., 2010). Ullah et al. (2016). Because of this, a plethora of

authentication approaches have been adopted to mitigate this issue. However, high levels of authentication are required to ensure confidence in securing the system against impersonation attacks. Due to these applied methods students may have concerns for continuously authenticating (Okada et. al., 2019).

Applying the framework utilizing the Unified Theory of Acceptance and Use of Technology Model (UTAUT), the objective of this research was to find out how student concerns for continuous authentication technologies, such as lock-down browsers, web-cam monitoring, or proctoring systems would affect students' attitudes and intentions to use the technology during an e-exam. The UTAUT model has been used as a scientific paradigm for understanding acceptance and use of learning technologies. In addition, this method has been found to explain the relationship between performance and effort expectancy towards using systems, as well as attitudes and intentions to use systems. Some studies that employed this model have also tested trust and perceived risks as constructs that were found to be associated with predicting behavioral intentions and attitudes towards using technologies.

This study was undertaken because there was an inclination that students may distrust or reject continuous authentication systems (such as webcam monitoring technologies, proctoring and lock-down browser systems) due to concerns that arise for the authentication method while taking an exam. Therefore, this research aimed to answer the question of whether student concerns for continuous authentication methods applied to mitigate impersonation attacks may affect their attitudes and intentions to use the technology during an e-exam.

The study looked at student concerns for continuous authentication methods through analysis of the associated constructs found within the literature including performance expectancy, effort expectancy, privacy concerns and how these constructs may impact attitudes

towards the system and behavioral intentions to use the system and the study also examined how trust or perceived risks are associated with these concerns. A review of the literature, which is subsequently highlighted, provided background and an understanding of the related constructs.

Behavioral intentions refer to the intent for the learners to employ e-learning systems and persistently use the technology from the present to the future (Salloum et al., 2019). Acceptability of e-authentication is an important issue because authentication is impractical if users deny or find it unacceptable, (Laamaen et al. 2021). Due to this significance, research employs behavioral intention as a key dependent variable to better understand and predict usage behaviors (Venkatesh et al., 2003). Another key dependent variable found within the literature is attitude but has also been found to directly affect behavioral intentions to use certain technologies (Salloum et al., 2019).

Attitude reflects the degree of positivity or negativity that a person feels towards an object (Lavrakas, 2008). Prior studies have also used attitudes as a key dependent variable and related attitude to behavioral intentions to using systems. In the context of testing attitudes towards e-learning mechanisms, the literature, findings indicate that attitude plays a significant role in persuading student intentions to use or accept technologies within e-learning systems (Hussein, 2017). In brief, the literature uncovered that attitude exerts a direct influence on intentions to use systems. Scholarly research also related attitude to performance expectancy, effort expectancy and privacy concerns.

This study uncovered a significant direct correlational relationship between student attitudes and their behavioral intentions to use the technology. The results of this research also suggest that there is a positive association between attitudes and intentions to use each system. Therefore, as positive attitudes increase behavioral intentions to use the system increases as

well. This study also looked at how attitudes and behavioral are influenced by performance expectancy, effort expectancy, and privacy concerns, and how this association is related to trust in the technology and perceived risks for the system.

It was found within the literature that performance expectancy was deemed to be important because attitudes regarding performance may influence a student's academic work when using authentication technologies during an exam (Cakir & Solak, 2015). Performance expectancy refers to the perceptions of the end-user on improving (or declining) performance and increasing (or decreasing) efficiency achieved through use of the e-learning technology (Abdou & Jasimuddin, 2020). Within the context of e-examinations, grades and academic achievement are tied to performance. Performance expectancy was found to be one of the strongest determinants of behavioral intentions to use a system, especially in mandatory settings such as a required e-exam (Venkatesh et al., 2003; Wang et al., 2009). This research suggests that performance expectancy has a significant influence on students' attitudes and behavioral intentions on to use the system when they are required to continuously authenticate.

Effort expectancy stems from the beliefs that the system takes free mental effort to use (Alowayr, 2021). The literature found that there are authentication technologies that take mental effort while taking an e-exam. Like performance expectations, effort expectancy was also found to be significant in mandatory settings (Vankatesh et al., 2003). Prior research also suggested that effort expectancy is also a good predictor of intentions to use e-learning technologies (Abdou & Jasimuddin, 2020). Essentially, the authors argue that students would want to use systems that are simple and easy to access. This research suggests that this is the case, as for all three continuous authentication methods examined, students' expectations about how much effort it would take to use the system was found to have a significant effect on both their attitudes towards using the system, and their behavioral intentions to use the system.



Okada et al. (2019) found privacy concerns to be an imperative factor that is important to the use and acceptance of authentication approaches. A perceived need for privacy, security and physical invasiveness are attitude factors that may heavily influence intentions to use a system (James et al., 2008). The literature reveals that privacy concerns are associated with elevated levels of perceived risks (Miltgen et al., 2013). Prior research associate user acceptance of authentication systems, such as biometric technology, to privacy, trust and perceived risks. It was confirmed within the literature that trust creates an environment that is conducive to technology acceptance. It was also found that trust is an essential factor in reducing uncertainty, risk factors, and ensuring a sense of safety and is necessary for accepting a system by reducing perceived risks (Miltgen et al., 2013).

This study found that higher privacy concerns are associated with higher perceived risks which are, in turn, positively associated with behavioral and intentions to use the authentication method and attitudes towards an authentication technology. As students' privacy concerns increase, they perceive more risks associated with the authentication technology, and they would in turn form negative intentions to engage in the system and would have negative attitudes about the system. In addition, levels of trust were found to have a varying effect based on authentication method. Trust was found as a moderating factor for proctoring systems but not for webcam monitoring or lock-down browsers.

In summary, applying a framework from the UTAUT model, the following primary research question was addressed: How does student concerns for continuous authentication methods applied to mitigate impersonation attacks affect students' attitudes and intentions to use the technology during an e-exam? Essentially, the application of the UTAUT model and data analysis applied through multivariate methods helped to address this question. Findings suggests that students' perceptions indicate that performance expectancy, effort expectancy

and privacy concerns for continuous authentication may significantly influence their attitudes and behavioral intentions to use the technology during an e-exam and trust may act as a moderating factor, depending on the technology. Specifically, the findings in this research suggest that performance expectancy, effort expectancy and privacy concerns significantly influence a student's behavioral intentions to use the system and their attitudes towards any of the continuous authentication systems examined for this research. The study also finds that students' privacy concerns are positively associated with their perceived risks for the technology. If privacy concerns increase, then perceived risks or uncertainties in the technology also increase. Sequentially, if students have increased perceived risks for the technology, then their behavioral intentions and attitudes will also be negatively affected. An increase in perceived risks or uncertainty for the system may result in a decrease in positive attitudes and students may have a negative behavioral intent to use the system in the future. Findings also imply that for proctoring systems, privacy concerns can indirectly influence attitudes and behavioral intentions indirectly through perceived risks and this mediation is moderated by an increase or decrease in trust. The finding has implications for training invigilation staff to ensure that students have less perceived risks about authenticating while they are being proctored.

Beyond the purview of this investigation, it was also found that for web-cam monitoring and lock-down browsers, although privacy concerns had an indirect effect on behavioral intentions through perceived risks, privacy concerns also had a directly negative effect on behavioral intentions to use the authentication methods. Further investigation and future research can examine how the levels of authentication for each technology are associated with these findings. The results of this study stress the importance of understanding student perspectives to shape their experiences with continuous authentication technologies.

## Appendices

## Appendix A. Nova IRB Approval

### MEMORANDUM

To: Andrea Green  
College of Engineering and Computing

From: Ling Wang, Ph.D.  
College Representative, College of Engineering and Computing

Date: August 31, 2022

Subject: IRB Exempt Initial Approval Memo

TITLE: Student Attitudes and Intentions to Use Continuous Authentication Methods Applied to Mitigate Impersonation Attacks During E-Assessments– NSU IRB Protocol Number 2022-398

Dear Principal Investigator,

Your submission has been reviewed and Exempted by your IRB College Representative or their Alternate on **August 31, 2022**. You may proceed with your study.

*Please Note: Exempt studies do not require approval stamped documents. If your study site requires stamped copies of consent forms, recruiting materials, etc., contact the IRB Office.*

**Level of Review:** Exempt

**Type of Approval:** Initial Approval

**Exempt Review Category:** Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies

**Post-Approval Monitoring:** The IRB Office conducts post-approval review and monitoring of all studies involving human participants under the purview of the NSU IRB. The Post-Approval Monitor may randomly select any active study for a Not-for-Cause Evaluation.

**Annual Status of Research Update:** You are required to notify the IRB Office annually if your research study is still ongoing via the *Exempt Research Status Update xForm*.

**Final Report:** You are required to notify the IRB Office within 30 days of the conclusion of the research that the study has ended using the *Exempt Research Status Update Form*.

**Translated Documents:** No

*Please retain this document in your IRB correspondence file.*

CC: Ling Wang, Ph.D.

Ling Wang, Ph.D.

## Appendix B. FIU IRB Approval



Office of Research Integrity  
Research Compliance, MARC 414

### MEMORANDUM

**To:** Dr. Dionne Stephens  
**CC:** Andrea Green  
**From:** Maria Melendez-Vargas, MIBA, IRB Coordinator  
**Date:** January 9, 2023  
**Protocol Title:** "Authentication & E-Assessments"

W

The Social and Behavioral Institutional Review Board of Florida International University has approved your study for the use of human subjects via the **Expedited Review** process. Your study was found to be in compliance with this institution's Federal Wide Assurance (00000060).

<b>IRB Protocol Approval #:</b>	IRB-22-0541	<b>IRB Approval Date:</b>	12/22/22
<b>TOPAZ Reference #:</b>	112205	<b>IRB Expiration Date:</b>	12/22/25

As a requirement of IRB Approval you are required to:

- 1) Submit an IRB Amendment Form for all proposed additions or changes in the procedures involving human subjects. All additions and changes must be reviewed and approved by the IRB prior to implementation.
- 2) Promptly submit an IRB Event Report Form for every serious or unusual or unanticipated adverse event, problems with the rights or welfare of the human subjects, and/or deviations from the approved protocol.
- 3) Utilize copies of the date stamped consent document(s) for obtaining consent from subjects (unless waived by the IRB). Signed consent documents must be retained for at least three years after the completion of the study.
- 4) **Receive annual review and re-approval of your study prior to your IRB expiration date.** Submit the IRB Renewal Form at least 30 days in advance of the study's expiration date.
- 5) Submit an IRB Project Completion Report Form when the study is finished or discontinued.

**HIPAA Privacy Rule:** N/A

**Special Conditions:** N/A

For further information, you may visit the IRB website at <http://research.fiu.edu/irb>.

MMV/em



**INSTITUTIONAL REVIEW BOARD**  
3301 College Avenue  
Fort Lauderdale, Florida 33314-7796  
PHONE: (954) 262-5369

### **Participant Letter for Anonymous Surveys**

#### **NSU Consent to be in a Research Study Entitled**

*Student Attitudes and Intentions to Use Continuous Authentication Methods Applied to Mitigate Impersonation Attacks During E-Assessments*

#### **Who is doing this research study?**

This person doing this study is Andrea Green with the College of Computing and Engineering. They will be helped by Dr. Ling Wang, Faculty Advisor.

#### **Why are you asking me to be in this research study?**

You are being asked to take part in this research study because you are an undergraduate student at FIU who may have taken an e-exam in one of your courses and was required to authenticate using a proctoring service, video-web cam monitoring, a lock-down browser or biometric equipment.

#### **Why is this research being done?**

The purpose of this study is to find out student attitudes and intentions to use e-assessment systems that uses methods (such as proctoring technology, video monitoring, lock-down browsers or biometric technology) to identify students prior to taking an exam to ensure identification of the student taking the exam.

#### **What will I be doing if I agree to be in this research study?**

You will be taking a one-time, anonymous survey. The survey will take approximately 30 minutes to 1 hour to complete.

#### **Are there possible risks and discomforts to me?**

This research study involves minimal risk to you. To the best of our knowledge, the things you will be doing have no more risk of harm than you would have in everyday life.

#### **What happens if I do not want to be in this research study?**

You can decide not to participate in this research and it will not be held against you. You can exit the survey at any time.

#### **Will it cost me anything? Will I get paid for being in the study?**

There is no cost for participation in this study. Participation is voluntary and no payment will be provided.



**INSTITUTIONAL REVIEW BOARD**  
3301 College Avenue  
Fort Lauderdale, Florida 33314-7796  
PHONE: (954) 262-5369

**How will you keep my information private?**

Your responses are anonymous. Information we learn about you in this research study will be handled in a confidential manner, within the limits of the law. Your name or any identifiable information about you will not be collected and will remain completely anonymous and will not be collected via the survey. This data will be available to the researcher, the Institutional Review Board and other representatives of this institution, and any granting agencies (if applicable). All confidential data will be kept securely and will be stored on a secured server and secured computer which only the researcher can access. All data will be kept for 36 months from the end of the study and destroyed after that time by means of deletion of the survey as well as deletion of any related information and documents stored on the researcher's computer.

**Who can I talk to about the study?**

If you have questions, you can contact Andrea Green at 305-348-6325 or 305-761-8890. Or the Faculty advisor Lin Wang can be contacted at 954-262-2020 or 1800-986-2247.

If you have questions about the study but want to talk to someone else who is not a part of the study, you can call the Nova Southeastern University Institutional Review Board (IRB) at (954) 262-5369 or toll free at 1-866-499-0790 or email at [IRB@nova.edu](mailto:IRB@nova.edu).

**Do you understand and do you want to be in the study?**

If you have read the above information and voluntarily wish to participate in this research study, please access the survey via Qualtrics by clicking on the following link:

[https://fiu.qualtrics.com/jfe/form/SV\\_2rdg8tVqoil8R2m](https://fiu.qualtrics.com/jfe/form/SV_2rdg8tVqoil8R2m)

## Appendix C. Survey Questionnaire

### Survey for Acceptance of E-Exam Authentication Methods

---

Start of Block: The following section provides us with basic information about you.

Year of Birth (write in your answer)

---

What is your sex?

- Male
- Female
- Non-binary / third gender
- Prefer not to say
- Other (please write in answer)

---



What is your primary racial identity?

- Asian
  - Black/ African descent
  - Hispanic/ Latin American
  - Indigenous/ Native
  - White non- Hispanic/ Caucasian
  - Other (please write in answer)
- 

What is your second racial identity?

- Not applicable
  - Asian
  - Black/ African descent
  - Hispanic/ Latin American
  - Indigenous/ Native
  - White non- Hispanic/ Caucasian
  - Other (please write in answer)
- 

What is your first familial national identity/ family homeland?

---

What is your second familial national identity/ family homeland?

---

How many years have you lived in the United States? (write in your answer)

---

What is the zip code of the place you consider to be home in the United States?

---

What is the zip code of your current place of residence?

---

What is the highest level of education completed by your mother?

- Some elementary school
  - Elementary school
  - Some high school
  - High school
  - Some college
  - Associates degree
  - Bachelor's degree
  - Some graduate school
  - Masters level degree
  - Doctoral level degree
-

What is the highest level of education completed by your father?

- Some elementary school
  - Elementary school
  - Some high school
  - High school
  - Some college
  - Associates degree
  - Bachelor's degree
  - Some graduate school
  - Masters level degree
  - Doctoral level degree
- 

What is your current class standing?

- Freshman
  - Sophomore
  - Junior
  - Senior
  - Grad Student
  - Other \_\_\_\_\_
-

Are YOU a parent with a son or daughter?

- Yes
- No

End of Block: The following section provides us with basic information about you.

---

Start of Block: Block 1



Which method of e-exam security were you ever required to use while taking an e-exam?

- Proctoring
- Lock-Down Browser
- Web-Cam Monitoring
- Biometric Technology (Fingerprint Verifier)
- Biometric Technology (Facial Recognition)

End of Block: Block 1

---

Start of Block: Survey for Acceptance of E-Exam Authentication Methods (Proctor-U)

An Online Proctoring System (example Proctor-U or Honor Lock) is an online system developed to secure an e-exam against cheating instances through the reliance of a hired and trained proctor who monitors the test taker throughout the exam. The proctor requests and verifies identification, scans the environment, explains the rules of the exam and then proceeds to monitor the test-taker via webcam and microphone throughout the exam. If any red-flags are detected the proctor would report the incident to the instructor. In certain instances, the proctor would discontinue the exam and report the incident to the instructor.

-----

**When taking an e-exam and being monitored by a Proctor. Please indicate the degree to which you agree or disagree with the following statements.**

	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
The e-authentication might not work properly during an e-exam.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The e-exam system might say I am cheating when I am not cheating.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The e-authentication might make the assessment take more time.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
It might be difficult to challenge the outcomes of e-authentication if the system questions my identity.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Using the e-authentication system increased my trust in my e-assessment.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The e-authentication can be intrusive.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I would fully trust authenticating (with proctoring) through an e-exam system.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

I trust that using the authentication method will be careful with my personal data.

I trust that my personal information will not be released to third parties

I believe that the authentication method is trustworthy

I trust the authentication and e-exam system

I am concerned that my data is shared with third parties without my agreement.

To authenticate, I have to share my personal data.

Using this authentication system during an e-exam makes me feel nervous about being monitored.

I feel that opening the e-authentication method during online exams is impractical and would breach my privacy.

The concern of using this e-authentication for me was privacy.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I have some concerns regarding recorded videos and pictures of me during my exams.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I feel like the e-authentication tools are invading my personal life and reducing my learning satisfaction.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am concerned about the privacy of my personal information while authenticating during the e-exam process.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I trust using the authentication method would be careful with my personal data.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I trust that my personal information will not be released to third parties	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Using the authentication system will reduce my effectiveness on the e-exam	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



Using the system would reduce my e-exam performance.

Using the authentication system would enable me to accomplish the e-exam task more quickly.

I lose time using the authentication method when taking an e-exam

The authentication method would decrease my productivity during the e-exam.

The authentication method would decrease my performance in the e-exam activity.

Using the authentication method would diminish my effectiveness on the e-exam activity.

Interacting with the authentication system is often frustrating when taking an e-exam.

When taking an e-exam, I believe that it is easy to use the authentication method.

I often become confused when I use the authentication system when taking an e-exam.

The authentication system is rigid and inflexible to interact with.

When taking an e-exam, I believe that it is easy to use the authentication method.

There is clarity and understanding in my interaction with the e-authentication technology.

The e-authentication system is easy to use for me.

Interacting with the e-authentication system does not require a lot of my mental effort.

Learning to operate the e-authentication system would be easy for me.

My interaction with the e-authentication technology would be clear and understandable.

The e-authentication method (proctoring) system is easy to use.

When taking an e-exam, it is probable that authenticating would frustrate me because of its poor performance.

I am worried about the use of the e-authentication method because people might have access to my data.

The likelihood that something wrong will happen with authentication while using the e-exam system is high.

Compared to other technologies, using the authentication method would have more uncertainties.

I feel apprehensive or uncomfortable about using the authentication method to accomplish my e-exam task.

I am satisfied with my experience of using the e-authentication system.

When I use the e-authentication system, I feel an increased level of surveillance than I usually experience when taking an e-exam.

When I use the e-exam system I felt more stressed than I usually do when taking an e-exam.

I think using the e-authentication tool as an authentication method is not at all effective.

I think using the e-authentication tool as an authentication method is not at all valuable.

I think using the e-authentication tool as an authentication method is bad.

I think using the e-authentication tool as an authentication method is not at all credible.

Overall, I like using the authentication method when taking an e-exam.

I will give out my recommendation to others to use the authentication method after an e-exam.

I think I am willing to try out the authentication method when taking the exam.

I would like to use the authentication method on a regular basis in the future.

I will not  
recommend to  
other students to  
use the  
authentication  
method.

I think  
authentication  
should be  
implemented in  
e-exams

A Lock-down browser is an online tool developed to secure an e-exam against cheating instances through a custom browser that is accessed on your computer to lock down the testing environment. Once you have accessed the lockdown browser, you are unable to access the internet and the software shuts down any programs or applications on your computer prior to beginning the e-exam. There may also be a webcam associated with some lock-down browser depending on the requirements set by the instructor. There is analytics applied to flag any violations during the exam.

---

**When taking an e-exam and being required to use a lock-down browser. Please indicate the degree to which you agree or disagree with the following statements**

	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
The e-authentication might not work properly during an e-exam.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The e-exam system might say I am cheating when I am not cheating.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The e-authentication might make the assessment take more time.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
It might be difficult to challenge the outcomes of e-authentication if the system questions my identity.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Using the e-authentication system increased my trust in my e-assessment.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The e-authentication can be intrusive.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I would fully trust authenticating (with a lock-down browser) through an e-exam system.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

I trust that using the authentication method will be careful with my personal data.

I trust that my personal information will not be released to third parties

I believe that the authentication method is trustworthy

I trust the authentication and e-exam system

I am concerned that my data is shared with third parties without my agreement.

To authenticate, I have to share my personal data.

Using this authentication system during an e-exam makes me feel nervous about being monitored.

I feel that opening the e-authentication method during online exams is impractical and would breach my privacy.



The concern of using this e-authentication for me was privacy.

I feel like the e-authentication tools are invading my personal life and reducing my learning satisfaction.

I am concerned about the privacy of my personal information while authenticating during the e-exam process.

I trust using the authentication method would be careful with my personal data.

I trust that my personal information will not be released to third parties

Using the authentication system will reduce my effectiveness on the e-exam

Using the system would reduce my e-exam performance.

Using the authentication system would enable me to accomplish the e-exam task more quickly.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I lose time using the authentication method when taking an e-exam	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The authentication method would decrease my productivity during the e-exam.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The authentication method would decrease my performance in the e-exam activity.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Using the authentication method would diminish my effectiveness on the e-exam activity.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Interacting with the authentication system is often frustrating when taking an e-exam.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
When taking an e-exam, I believe that it is easy to use the authentication method.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

I often become confused when I use the authentication system when taking an e-exam.

The authentication system is rigid and inflexible to interact with.

When taking an e-exam, I believe that it is easy to use the authentication method.

There is clarity and understanding in my interaction with the e-authentication technology.

The e-authentication system is easy to use for me.

Interacting with the e-authentication system does not require a lot of my mental effort.

Learning to operate the e-authentication system would be easy for me.

My interaction with the e-authentication technology would be clear and understandable.

The e-authentication method (lock-down browser) system is easy to use.

When taking an e-exam, it is probable that authenticating would frustrate me because of its poor performance.

I am worried about the use of the e-authentication method because people might have access to my data.

The likelihood that something wrong will happen with authentication while using the e-exam system is high.

Compared to other technologies, using the authentication method would have more uncertainties.

I feel apprehensive or uncomfortable about using the authentication method to accomplish my e-exam task.

I am satisfied with my experience of using the e-authentication system.

When I use the e-authentication system, I feel an increased level of surveillance than I usually experience when taking an e-exam.

When I use the e-exam system I felt more stressed than I usually do when taking an e-exam.

I think using the e-authentication tool as an authentication method is not at all effective.

I think using the e-authentication tool as an authentication method is not at all valuable.

I think using the e-authentication tool as an authentication method is bad.

I think using the e-authentication tool as an authentication method is not at all credible.

Overall, I like using the authentication method when taking an e-exam.

I will give out my recommendation to others to use the authentication method after an e-exam.

I think I am willing to try out the authentication method when taking the exam.

I would like to use the authentication method on a regular basis in the future.

I will not recommend to other students to use the authentication method.

I think authentication should be implemented in e-exams

Webcam monitoring is an authentication method used in conjunction with the Lockdown Browser. It uses the webcam and microphone to records test takers screen activities and testing behavior while they are taking the exam using Lockdown Browser. Instructors can view the recordings and review details of the testing process after the exam is submitted.

---

**When taking an e-exam whereby webcam monitoring is required: Please indicate the degree to which you agree or disagree with the following statements.**

	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
The e-authentication might not work properly during an e-exam.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The e-exam system might say I am cheating when I am not cheating.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The e-authentication might make the assessment take more time.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
It might be difficult to challenge the outcomes of e-authentication if the system questions my identity.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Using the e-authentication system increased my trust in my e-assessment.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The e-authentication can be intrusive.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I would fully trust authenticating (web-cam monitoring) through an e-exam system.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



I trust that using the authentication method will be careful with my personal data.

I trust that my personal information will not be released to third parties

I believe that the authentication method is trustworthy

I trust the authentication and e-exam system

I am concerned that my data is shared with third parties without my agreement.

To authenticate, I have to share my personal data.

Using this authentication system during an e-exam makes me feel nervous about being monitored.

I feel that opening the e-authentication method during online exams is impractical and would breach my privacy.

The concern of using this e-authentication for me was privacy.

I have some concerns regarding recorded videos and pictures of me during my exams.

I feel like the e-authentication tools are invading my personal life and reducing my learning satisfaction.

I am concerned about the privacy of my personal information while authenticating during the e-exam process.

I trust using the authentication method would be careful with my personal data.

I trust that my personal information will not be released to third parties

Using the authentication system will reduce my effectiveness on the e-exam

Using the system would reduce my e-exam performance.

Using the authentication system would enable me to accomplish the e-exam task more quickly.

I lose time using the authentication method when taking an e-exam

The authentication method would decrease my productivity during the e-exam.

The authentication method would decrease my performance in the e-exam activity.

Using the authentication method would diminish my effectiveness on the e-exam activity.

Interacting with the authentication system is often frustrating when taking an e-exam.

When taking an e-exam, I believe that it is easy to use the authentication method.

I often become confused when I use the authentication system when taking an e-exam.

The authentication system is rigid and inflexible to interact with.

When taking an e-exam, I believe that it is easy to use the authentication method.

There is clarity and understanding in my interaction with the e-authentication technology.

The e-authentication system is easy to use for me.

Interacting with the e-authentication system does not require a lot of my mental effort.

Learning to operate the e-authentication system would be easy for me.

My interaction with the e-authentication technology would be clear and understandable.

The e-authentication method (web-cam monitoring) system is easy to use.

When taking an e-exam, it is probable that authenticating would frustrate me because of its poor performance.

I am worried about the use of the e-authentication method because people might have access to my data.

The likelihood that something wrong will happen with authentication while using the e-exam system is high.

Compared to other technologies, using the authentication method would have more uncertainties.

I feel apprehensive or uncomfortable about using the authentication method to accomplish my e-exam task.

I am satisfied with my experience of using the e-authentication system.

When I use the e-authentication system, I feel an increased level of surveillance than I usually experience when taking an e-exam.

When I use the e-exam system I felt more stressed than I usually do when taking an e-exam.

I think using the e-authentication tool as an authentication method is not at all effective.

I think using the e-authentication tool as an authentication method is not at all valuable.

I think using the e-authentication tool as an authentication method is bad.

I think using the e-authentication tool as an authentication method is not at all credible.

Overall, I like using the authentication method when taking an e-exam.

I will give out my recommendation to others to use the authentication method after an e-exam.

I think I am willing to try out the authentication method when taking the exam.

I would like to use the authentication method on a regular basis in the future.

I will not  
recommend to  
other students to  
use the  
authentication  
method.

I think  
authentication  
should be  
implemented in  
e-exams

Biometric Technology (fingerprint verifier) is an authentication method used to secure exams by using hardware equipment (a finger-print scanner) which captures a finger-print or palm-print image using infrared light.

---

**When taking an e-exam whereby a fingerprint verifier is required: Please indicate the degree to which you agree or disagree with the following statements.**



	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
The e-authentication might not work properly during an e-exam.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The e-exam system might say I am cheating when I am not cheating.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The e-authentication might make the assessment take more time.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
It might be difficult to challenge the outcomes of e-authentication if the system questions my identity.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Using the e-authentication system increased my trust in my e-assessment.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The e-authentication can be intrusive.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I would fully trust authenticating (finger-print verifier) through an e-exam system.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

I trust that using the authentication method will be careful with my personal data.

I trust that my personal information will not be released to third parties

I believe that the authentication method is trustworthy

I trust the authentication and e-exam system

I am concerned that my data is shared with third parties without my agreement.

To authenticate, I have to share my personal data.

Using this authentication system during an e-exam makes me feel nervous about being monitored.

I feel that opening the e-authentication method during online exams is impractical and would breach my privacy.

The concern of using this e-authentication for me was privacy.

I feel like the e-authentication tools are invading my personal life and reducing my learning satisfaction.

I am concerned about the privacy of my personal information while authenticating during the e-exam process.

I trust using the authentication method would be careful with my personal data.

I trust that my personal information will not be released to third parties

Using the authentication system will reduce my effectiveness on the e-exam

Using the system would reduce my e-exam performance.

Using the authentication system would enable me to accomplish the e-exam task more quickly.

I lose time using the authentication method when taking an e-exam

The authentication method would decrease my productivity during the e-exam.

The authentication method would decrease my performance in the e-exam activity.

Using the authentication method would diminish my effectiveness on the e-exam activity.

Interacting with the authentication system is often frustrating when taking an e-exam.

When taking an e-exam, I believe that it is easy to use the authentication method.

I often become confused when I use the authentication system when taking an e-exam.

The authentication system is rigid and inflexible to interact with.

When taking an e-exam, I believe that it is easy to use the authentication method.

There is clarity and understanding in my interaction with the e-authentication technology.

The e-authentication system is easy to use for me.

Interacting with the e-authentication system does not require a lot of my mental effort.

Learning to operate the e-authentication system would be easy for me.

My interaction with the e-authentication technology would be clear and understandable.

The e-authentication method (fingerprint verifier) system is easy to use.

When taking an e-exam, it is probable that authenticating would frustrate me because of its poor performance.

I am worried about the use of the e-authentication method because people might have access to my data.

The likelihood that something wrong will happen with authentication while using the e-exam system is high.

Compared to other technologies, using the authentication method would have more uncertainties.

I feel apprehensive or uncomfortable about using the authentication method to accomplish my e-exam task.

I am satisfied with my experience of using the e-authentication system.

When I use the e-authentication system, I feel an increased level of surveillance than I usually experience when taking an e-exam.

When I use the e-exam system I felt more stressed than I usually do when taking an e-exam.

I think using the e-authentication tool as an authentication method is not at all effective.

I think using the e-authentication tool as an authentication method is not at all valuable.

I think using the e-authentication tool as an authentication method is bad.

I think using the e-authentication tool as an authentication method is not at all credible.

Overall, I like using the authentication method when taking an e-exam.

I will give out my recommendation to others to use the authentication method after an e-exam.

I think I am willing to try out the authentication method when taking the exam.

I would like to use the authentication method on a regular basis in the future.

I will not recommend to other students to use the authentication method.

I think authentication should be implemented in e-exams



Biometric Technology (facial recognition software) is an authentication method used to secure exams by using a deep learning algorithm to perform facial recognition through scans that identifies face-features to authenticate if the right candidate is being proctored.

---

**When taking an e-exam whereby a Biometric (face recognition software) is required:  
Please indicate the degree to which you agree or disagree with the following statements.**

	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
The e-authentication might not work properly during an e-exam.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The e-exam system might say I am cheating when I am not cheating.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The e-authentication might make the assessment take more time.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
It might be difficult to challenge the outcomes of e-authentication if the system questions my identity.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Using the e-authentication system increased my trust in my e-assessment.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The e-authentication can be intrusive.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I would fully trust authenticating (face recognition software) through an e-exam system.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

I trust that using the authentication method will be careful with my personal data.

I trust that my personal information will not be released to third parties

I believe that the authentication method is trustworthy

I trust the authentication and e-exam system

I am concerned that my data is shared with third parties without my agreement.

To authenticate, I have to share my personal data.

Using this authentication system during an e-exam makes me feel nervous about being monitored.

I feel that opening the e-authentication method during online exams is impractical and would breach my privacy.

The concern of using this e-authentication for me was privacy.

I feel like the e-authentication tools are invading my personal life and reducing my learning satisfaction.

I am concerned about the privacy of my personal information while authenticating during the e-exam process.

I trust using the authentication method would be careful with my personal data.

I trust that my personal information will not be released to third parties

Using the authentication system will reduce my effectiveness on the e-exam

Using the system would reduce my e-exam performance.

Using the authentication system would enable me to accomplish the e-exam task more quickly.

I lose time using the authentication method when taking an e-exam

The authentication method would decrease my productivity during the e-exam.

The authentication method would decrease my performance in the e-exam activity.

Using the authentication method would diminish my effectiveness on the e-exam activity.

Interacting with the authentication system is often frustrating when taking an e-exam.

When taking an e-exam, I believe that it is easy to use the authentication method.

I often become confused when I use the authentication system when taking an e-exam.

The authentication system is rigid and inflexible to interact with.

When taking an e-exam, I believe that it is easy to use the authentication method.

There is clarity and understanding in my interaction with the e-authentication technology.

The e-authentication system is easy to use for me.

Interacting with the e-authentication system does not require a lot of my mental effort.

Learning to operate the e-authentication system would be easy for me.

My interaction with the e-authentication technology would be clear and understandable.

The e-authentication method (face recognition software) system is easy to use.

When taking an e-exam, it is probable that authenticating would frustrate me because of its poor performance.

I am worried about the use of the e-authentication method because people might have access to my data.

The likelihood that something wrong will happen with authentication while using the e-exam system is high.

Compared to other technologies, using the authentication method would have more uncertainties.

I feel apprehensive or uncomfortable about using the authentication method to accomplish my e-exam task.

I am satisfied with my experience of using the e-authentication system.

When I use the e-authentication system, I feel an increased level of surveillance than I usually experience when taking an e-exam.

When I use the e-exam system I felt more stressed than I usually do when taking an e-exam.

I think using the e-authentication tool as an authentication method is not at all effective.

I think using the e-authentication tool as an authentication method is not at all valuable.

I think using the e-authentication tool as an authentication method is bad.



I think using the e-authentication tool as an authentication method is not at all credible.

Overall, I like using the authentication method when taking an e-exam.

I will give out my recommendation to others to use the authentication method after an e-exam.

I think I am willing to try out the authentication method when taking the exam.

I would like to use the authentication method on a regular basis in the future.

I will not recommend to other students to use the authentication method.

I think authentication should be implemented in e-exams

---

**Start of Block: Block 3**

If you believe you may need resources and support for testing anxiety or high levels of stress felt during testing, please contact the DRC: Disability Resource Center at 305-348-3532.

CAPS: Counseling and Psychological Services can also provide support. Please reach out to them at 305-348-2277.

## Appendix D. Variance Factor Scores

*Variance Factor Scores: VIF Values using SPSS:*

Model	Unstandardized Coefficients		Standard Coefficients		Collinearity Statistics		
	B	Std. Error	Beta	t	Sig.	Tolerance	VIF
(Constant)	23.538	0.241		97.654	0		
PC	-1.306	0.278	-0.203	-4.695	<.001	0.825	1.212
PE	-1.302	0.278	-0.202	-4.679	<.001	0.825	1.212
EE	1.749	0.254	0.27	6.885	<.001	1	1

*Note.* Dependent Variable: Proctoring-AT

Model	Unstandardized Coefficients		Standard Coefficients		Collinearity Statistics		
	B	Std. Error	Beta	t	Sig.	Tolerance	VIF
(Constant)	18.609	0.337		55.237	<.001		
PC	-2.165	0.388	-0.237	-5.582	<.001	0.826	1.21
PE	-2.152	0.388	-0.236	-5.547	<.001	0.826	1.21
EE	2.104	0.354	0.229	5.937	<.001	1	1

*Note.* Dependent Variable: Proctoring- BI

Model	Unstandardized Coefficients		Standard Coefficients		Collinearity Statistics		
	B	Std. Error	Beta	t	Sig.	Tolerance	VIF
(Constant)	23.676	0.302		78.484	<.001		
PC	-0.948	0.343	-0.146	-2.764	0.006	0.813	1.23
PE	-1.43	0.343	-0.22	-4.166	<.001	0.813	1.23
EE	1.448	0.315	0.218	4.592	<.001	1	1

*Note.* Dependent Variable: WCM-AT

Model	Unstandardized Coefficients		Standard Coefficients		Collinearity Statistics		
	B	Std. Error	Beta	t	Sig.	Tolerance	VIF
(Constant)	20.137	0.385		52.316	<.001		
PC	-3.501	0.437	-0.379	-8.018	<.001	0.808	1.237
PE	-2.221	0.436	-0.241	-5.088	<.001	0.808	1.237
EE	1.315	0.4	0.14	3.284	0.001	1	1

*Note.* Dependent Variable: WCM- BI

*Variance Factor Scores: VIF Values using SPSS:*

Model	Unstandardized Coefficients		Standard Coefficients			Collinearity Statistics	
	B	Std. Error	Beta	t	Sig.	Tolerance	VIF
(Constant)	22.937	0.235		97.483	0		
PC	-0.895	0.271	-0.139	-3.297	0.001	0.779	1.283
PE	-1.139	0.273	-0.176	-4.166	<.001	0.775	1.29
EE	1.439	0.245	0.22	5.874	<.001	0.994	1.006

*Note.* Dependent Variable: LDB - AT

Model	Unstandardized Coefficients		Standard Coefficients			Collinearity Statistics	
	B	Std. Error	Beta	t	Sig.	Tolerance	VIF
(Constant)	-2.511	0.379	-0.263	-6.617	<.001	0.784	1.275
PC	-2.392	0.382	-0.249	-6.26	<.001	0.78	1.281
PE	1.593	0.344	0.163	4.634	<.001	0.994	1.006
EE	-2.511	0.379	-0.263	-6.617	<.001	0.784	1.275

*Note.* Dependent Variable: LDB - BI

## Appendix E. Equality Covariance Matrices

### *Box's M Test of Equality of Co-Variance Matrices*

Technology		Box's M	F	<i>df1</i>	<i>df2</i>	<i>sig</i>
Proctoring						
	IV-PC	1.78	.587	3	52430850.770	.624
	IV-PE	1.206	.400	3	59496875.426	.753
	IV-EE	3.593	1.193	3	1984810888.9	.311

*Note.* DVs are BI and AT; The Box's M test of covariance matrices tests that the covariance matrices of the dependent variables are equal across groups

Technology		Box's M	F	<i>df1</i>	<i>df2</i>	<i>sig</i>
Web-Cam Monitoring						
	IV-PC	1.958	.649	3	238346428.529	.583
	IV-PE	2.180	.723	3	29636050.113	.538
	IV-EE	9.23	3.089	3	6134958.071	.026

*Note.* DVs are BI and AT; The Box's M test of covariance matrices tests that the covariance matrices of the dependent variables are equal across groups

Technology		Box's M	F	<i>df1</i>	<i>df2</i>	<i>sig</i>
Lock-Down Browser						
	IV-PC	4.860	1.615	3	8956536.914	.184
	IV-PE	.688	.229	3	242220649.69	.876
	IV-EE	10.165	3.376	3	17933928.095	.017

*Note.* DVs are BI and AT; The Box's M test of covariance matrices tests that the covariance matrices of the dependent variables are equal across groups

## Appendix F Test of Equality of Error Variances

### *Levene's Test of Equality of Error Variances*

#### *Proctoring*

IV-DV PROC	Test Base	Levene Statistic	df1	df2	Sig.
PC-AT	N/A	.285	1	532	.594
PC- BI	N/A	.406	1	532	.524
PE- AT	Based on Mean	0.956	1	558	0.329
	Based on Median	1.01	1	558	0.315
	Median adjusted df	1.01	1	557.643	0.315
	Trimmed Mean	1.03	1	558	0.311
PE- BI	Based on Mean	0.699	1	558	0.403
	Based on Median	0.825	1	558	0.364
	Median adjusted df	0.825	1	539.448	0.364
	Trimmed Mean	0.545	1	558	0.46
EE-AT	Based on Mean	0.014	1	545	0.907
	Based on Median	0.017	1	545	0.895
	Median adjusted df	0.017	1	544.629	0.895
	Trimmed Mean	0.006	1	545	0.94
EE-BI	Based on Mean	0.001	1	545	0.982
	Based on Median	0.001	1	545	0.971
	Median adjusted df	0.001	1	538.231	0.971
	Trimmed Mean	0.001	1	545	0.97

*Note.* Levene's Test of Equality of Error Variances tests the null hypothesis that the error variance of the dependent variable is equal across groups

#### *Web-Cam Monitoring*

IV-DV WCM	Test Base	Levene Statistic	df1	df2	Sig.
PC-AT	N/A	0.62	1	386	.803
PC- BI	N/A	2.411	1	386	.121
PE- AT	Based on Mean	0.015	1	400	0.903
	Based on Median	0.003	1	400	0.959
	Median adjusted df	0.003	1	397.985	0.959
	Trimmed Mean	0.01	1	400	0.921
PE- BI	Based on Mean	2.316	1	400	0.129
	Based on Median	2.437	1	400	0.119
	Median adjusted df	2.437	1	396.082	0.119
	Trimmed Mean	2.038	1	400	0.154

EE-AT	Based on Mean	4.126	1	391	0.043
	Based on Median	3.693	1	391	0.055
	Median adjusted df	3.693	1	389.562	0.055
	Trimmed Mean	4.245	1	391	0.04
EE-BI	Based on Mean	2.415	1	391	0.121
	Based on Median	2.147	1	391	0.144
	Median adjusted df	2.147	1	369.469	0.144
	Trimmed Mean	2.296	1	391	0.131

*Note.* Levene's Test of Equality of Error Variances tests the null hypothesis that the error variance of the dependent variable is equal across groups.

### *Lock-Down Browser*

IV-DV		Levene	df1	df2	Sig.
LDB		Statistic			
PC-AT	N/A	1.419	1	647	.234
PC- BI	N/A	2.289	1	647	.131
PE- AT	Based on Mean	1.121	1	666	0.29
	Based on Median	1.049	1	666	0.306
	Median adjusted df	1.049	1	665.999	0.306
	Trimmed Mean	1.047	1	666	0.307
PE- BI	Based on Mean	3.328	1	666	0.069
	Based on Median	3.08	1	666	0.08
	Median adjusted df	3.08	1	635.436	0.08
	Trimmed Mean	3.335	1	666	0.068
EE-AT	Based on Mean	5.123	1	657	0.024
	Based on Median	5.349	1	657	0.021
	Median adjusted df	5.349	1	651.56	0.021
	Trimmed Mean	4.965	1	657	0.026
EE-BI	Based on Mean	0.002	1	657	0.962
	Based on Median	0.017	1	657	0.898
	Median adjusted df	0.017	1	656.975	0.898
	Trimmed Mean	0.007	1	657	0.935

*Note.* Levene's Test of Equality of Error Variances tests the null hypothesis that the error variance of the dependent variable is equal across groups.

**Appendix G. Reliability Statistics**

Proctoring		
Variable:	Cronbach's Alpha	<i>N</i> of Items
PROC-TR	0.611	11
PROC-PC	0.728	10
PROC-PE	0.878	7
PROC-EE	0.657	12
PROC-PR	0.853	4
PROC-AT	0.583	8
PROC-BI	0.607	5

Lock-Down Browser		
Variable:	Cronbach's Alpha	<i>N</i> of Items
LDB-TR	0.611	11
LDB-PC	0.728	10
LDB-PE	0.878	7
LDBEE	0.657	12
LDB-PR	0.853	4
LDB-AT	0.583	8
LDB-BI	0.607	5

Web-Cam Monitoring		
Variable:	Cronbach's Alpha	<i>N</i> of Items
WCM-TR	0.611	11
WCM-PC	0.728	10
WCM-PE	0.878	7
WCM-EE	0.657	12
WCM-PR	0.853	4
WCM-AT	0.583	8
WCM-BI	0.607	5



## Appendix H. Pearson Correlations

### Correlations among Proctoring Variables

	1	2	3	4	5	6
1. AT						
2. BI	.526**					
3. TR	.265**	.252**				
4. PC	-.275**	-.319**	-.092*			
5. PE	-.275**	-.310**	0.001	.415**		
6. EE	.257**	.217**	.189**	0.016	0.022	
7. PR	-.423**	-.450**	-.226**	.572**	.459**	0.001

Note. \* $N \leq 414$  \*\*  $p < 0.01$  level (2-tailed), \*  $p < 0.05$  level (2-tailed)

### Correlations among Web-Cam Monitoring Variables

	1	2	3	4	5	6
1. AT						
2. BI	.542**					
3. TR	.203**	.183**				
4. PC	-.232**	-.485**	0.001			
5. PE	-.265**	-.404**	0.024	.438**		
6. EE	.221**	.141**	.198**	0.002	0.011	
7. PR	-.390**	-.535**	-.100*	.629**	.502**	-0.079

Note. \* $N \leq 414$  \*\*  $p < 0.01$  level (2-tailed), \*  $p < 0.05$  level (2-tailed)

### Correlations among Lock-Down Browser Variables

	1	2	3	4	5	6
1. AT						
2. BI	.533**					
3. TR	.181**	.179**				
4. PC	-.225**	-.370**	-0.019			
5. PE	-.228**	-.358**	0.057	.464**		
6. EE	.202**	.145**	.126**	0.032	.084*	
7. PR	-.402**	-.541**	-.130**	.596**	.511**	0.032

Note. \* $N \leq 414$  \*\*  $p < 0.01$  level (2-tailed), \*  $p < 0.05$  level (2-tailed)

\*The total sample size varied across survey items and technologies.

## Appendix I. Multivariate Tests (MANOVA)

Multivariate Tests <sup>a</sup>									
Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power <sup>c</sup>
Intercept	Pillai's Trace	.982	15544.644 <sup>b</sup>	2.000	557.000	.000	.982	31089.287	1.000
	Wilks'	.018	15544.644 <sup>b</sup>	2.000	557.000	.000	.982	31089.287	1.000
	Lambda								
	Hotelling's Trace	55.816	15544.644 <sup>b</sup>	2.000	557.000	.000	.982	31089.287	1.000
	Roy's Largest Root	55.816	15544.644 <sup>b</sup>	2.000	557.000	.000	.982	31089.287	1.000
PROC_PE	Pillai's Trace	.112	35.267 <sup>b</sup>	2.000	557.000	<.001	.112	70.535	1.000
	Wilks'	.888	35.267 <sup>b</sup>	2.000	557.000	<.001	.112	70.535	1.000
	Lambda								
	Hotelling's Trace	.127	35.267 <sup>b</sup>	2.000	557.000	<.001	.112	70.535	1.000
	Roy's Largest Root	.127	35.267 <sup>b</sup>	2.000	557.000	<.001	.112	70.535	1.000

a. Design: Intercept + PROC\_PE b. Exact statistic c. Computed using alpha = .05

Tests of Between-Subjects Effects									
Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power <sup>c</sup>
Corrected Model	Proc_AT	438.327 <sup>a</sup>	1	438.327	45.438	<.001	.075	45.438	1.000
	Proc_BI	1111.471 <sup>b</sup>	1	1111.471	58.907	<.001	.095	58.907	1.000
Intercept	Proc_AT	299452.327	1	299452.327	31042.232	.000	.982	31042.232	1.000
	Proc_BI	169986.764	1	169986.764	9009.110	.000	.942	9009.110	1.000
PROC_PE	Proc_AT	438.327	1	438.327	45.438	<.001	.075	45.438	1.000
	Proc_BI	1111.471	1	1111.471	58.907	<.001	.095	58.907	1.000
Error	Proc_AT	5382.809	558	9.647					
	Proc_BI	10528.522	558	18.868					
Total	Proc_AT	304920.000	560						
	Proc_BI	181116.000	560						
Corrected Total	Proc_AT	5821.136	559						
	Proc_BI	11639.993	559						

a. R Squared = .075 (Adjusted R Squared = .074) b. R Squared = .095 (Adjusted R Squared = .094) c. Computed using alpha = .05

Multivariate Tests<sup>a</sup>

Effect		Value	F	Hypothesis		Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power <sup>c</sup>
				df	Error df				
Intercept	Pillai's Trace	.982	15126.217 <sup>b</sup>	2.000	544.000	.000	.982	30252.434	1.000
	Wilks' Lambda	.018	15126.217 <sup>b</sup>	2.000	544.000	.000	.982	30252.434	1.000
	Hotelling's Trace	55.611	15126.217 <sup>b</sup>	2.000	544.000	.000	.982	30252.434	1.000
	Roy's Largest Root	55.611	15126.217 <sup>b</sup>	2.000	544.000	.000	.982	30252.434	1.000
PROC_ EE	Pillai's Trace	.073	21.284 <sup>b</sup>	2.000	544.000	<.001	.073	42.567	1.000
	Wilks' Lambda	.927	21.284 <sup>b</sup>	2.000	544.000	<.001	.073	42.567	1.000
	Hotelling's Trace	.078	21.284 <sup>b</sup>	2.000	544.000	<.001	.073	42.567	1.000
	Roy's Largest Root	.078	21.284 <sup>b</sup>	2.000	544.000	<.001	.073	42.567	1.000

a. Design: Intercept + PROC\_EE b. Exact statistic c. Computed using alpha = .05

## Tests of Between-Subjects Effects

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power <sup>c</sup>
Corrected Model	Proc_AT	360.211 <sup>a</sup>	1	360.211	37.753	<.001	.065	37.753	1.000
	Proc_BI	480.009 <sup>b</sup>	1	480.009	24.516	<.001	.043	24.516	.999
Intercept	Proc_AT	288735.327	1	288735.327	30261. 977	.000	.982	30261.977	1.000
	Proc_BI	164250.174	1	164250.174	8389.0 83	.000	.939	8389.083	1.000
PROC_EE	Proc_AT	360.211	1	360.211	37.753	<.001	.065	37.753	1.000
	Proc_BI	480.009	1	480.009	24.516	<.001	.043	24.516	.999
Error	Proc_AT	5199.950	545	9.541					
	Proc_BI	10670.576	545	19.579					
Total	Proc_AT	298476.000	547						
	Proc_BI	178337.000	547						
Corrected Total	Proc_AT	5560.161	546						
	Proc_BI	11150.585	546						

a. R Squared = .065 (Adjusted R Squared = .063) b. R Squared = .043 (Adjusted R Squared = .041) c. Computed using alpha = .05

Multivariate Tests<sup>a</sup>

Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power <sup>c</sup>
Intercept	Pillai's Trace	.983	11369.988 <sup>b</sup>	2.000	399.000	.000	.983	22739.975	1.000
	Wilks' Lambda	.017	11369.988 <sup>b</sup>	2.000	399.000	.000	.983	22739.975	1.000
	Hotelling's Trace	56.992	11369.988 <sup>b</sup>	2.000	399.000	.000	.983	22739.975	1.000
	Roy's Largest Root	56.992	11369.988 <sup>b</sup>	2.000	399.000	.000	.983	22739.975	1.000
WCM_PE	Pillai's Trace	.170	40.799 <sup>b</sup>	2.000	399.000	<.001	.170	81.597	1.000
	Wilks' Lambda	.830	40.799 <sup>b</sup>	2.000	399.000	<.001	.170	81.597	1.000
	Hotelling's Trace	.205	40.799 <sup>b</sup>	2.000	399.000	<.001	.170	81.597	1.000
	Roy's Largest Root	.205	40.799 <sup>b</sup>	2.000	399.000	<.001	.170	81.597	1.000

## Tests of Between-Subjects Effects

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Square d	Noncent. Parameter	Observed Power <sup>c</sup>
Corrected Model	WCM_AT	313.855 <sup>a</sup>	1	313.855	32.249	<.001	.075	32.249	1.000
	WCM_BI	1393.778 <sup>b</sup>	1	1393.778	79.486	<.001	.166	79.486	1.000
Intercept	WCM_AT	219579.168	1	219579.168	22562.339	.000	.983	22562.339	1.000
	WCM_BI	131705.112	1	131705.112	7511.003	<.001	.949	7511.003	1.000
WCM_PE	WCM_AT	313.855	1	313.855	32.249	<.001	.075	32.249	1.000
	WCM_BI	1393.778	1	1393.778	79.486	<.001	.166	79.486	1.000
Error	WCM_AT	3892.844	400	9.732					
	WCM_BI	7013.983	400	17.535					
Total	WCM_AT	223587.000	402						
	WCM_BI	139738.000	402						
Corrected Total	WCM_AT	4206.699	401						
	WCM_BI	8407.761	401						

a. R Squared = .075 (Adjusted R Squared = .072) b. R Squared = .166 (Adjusted R Squared = .164) c. Computed using alpha = .05

Multivariate Tests<sup>a</sup>

Effect		Value	F	Hypothesis		Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power <sup>c</sup>
				df	Error df				
Intercept	Pillai's Trace	.981	10111.69 7 <sup>b</sup>	2.000	390.000	.000	.981	20223.394	1.000
	Wilks' Lambda	.019	10111.69 7 <sup>b</sup>	2.000	390.000	.000	.981	20223.394	1.000
	Hotelling's Trace	51.855	10111.69 7 <sup>b</sup>	2.000	390.000	.000	.981	20223.394	1.000
	Roy's Largest Root	51.855	10111.69 7 <sup>b</sup>	2.000	390.000	.000	.981	20223.394	1.000
WCM_EE	Pillai's Trace	.047	9.658 <sup>b</sup>	2.000	390.000	<.001	.047	19.316	.981
	Wilks' Lambda	.953	9.658 <sup>b</sup>	2.000	390.000	<.001	.047	19.316	.981
	Hotelling's Trace	.050	9.658 <sup>b</sup>	2.000	390.000	<.001	.047	19.316	.981
	Roy's Largest Root	.050	9.658 <sup>b</sup>	2.000	390.000	<.001	.047	19.316	.981

a. Design: Intercept + WCM\_EE b. Exact statistic c. Computed using alpha = .05

## Tests of Between-Subjects Effects

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power <sup>c</sup>
Corrected Model	WCM_AT	191.962 <sup>a</sup>	1	191.962	19.158	<.001	.047	19.158	.992
	WCM_BI	155.750 <sup>b</sup>	1	155.750	7.419	.007	.019	7.419	.776
Intercept	WCM_AT	203160.633	1	203160.633	20275.22 5	.000	.981	20275.225	1.000
	WCM_BI	121918.499	1	121918.499	5807.379	<.001	.937	5807.379	1.000
WCM_EE	WCM_AT	191.962	1	191.962	19.158	<.001	.047	19.158	.992
	WCM_BI	155.750	1	155.750	7.419	.007	.019	7.419	.776
Error	WCM_AT	3917.876	391	10.020					
	WCM_BI	8208.545	391	20.994					
Total	WCM_AT	218450.000	393						
	WCM_BI	137249.000	393						
Corrected Total	WCM_AT	4109.837	392						
	WCM_BI	8364.295	392						

a. R Squared = .047 (Adjusted R Squared = .044) b. R Squared = .019 (Adjusted R Squared = .016) c. Computed using alpha = .05

**Multivariate Tests<sup>a</sup>**

Effect		Value	F	Hypothesis		Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power <sup>c</sup>
				df	Error df				
Intercept	Pillai's Trace	.981	17291.579 <sub>b</sub>	2.000	665.000	.000	.981	34583.157	1.000
	Wilks' Lambda	.019	17291.579 <sub>b</sub>	2.000	665.000	.000	.981	34583.157	1.000
	Hotelling's Trace	52.005	17291.579 <sub>b</sub>	2.000	665.000	.000	.981	34583.157	1.000
	Roy's Largest Root	52.005	17291.579 <sub>b</sub>	2.000	665.000	.000	.981	34583.157	1.000
LDB_PE	Pillai's Trace	.132	50.446 <sup>b</sup>	2.000	665.000	<.001	.132	100.892	1.000
	Wilks' Lambda	.868	50.446 <sup>b</sup>	2.000	665.000	<.001	.132	100.892	1.000
	Hotelling's Trace	.152	50.446 <sup>b</sup>	2.000	665.000	<.001	.132	100.892	1.000
	Roy's Largest Root	.152	50.446 <sup>b</sup>	2.000	665.000	<.001	.132	100.892	1.000

a. Design: Intercept + LDB\_PE b. Exact statistic c. Computed using alpha = .05

**Tests of Between-Subjects Effects**

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power <sup>c</sup>
Corrected Model	LDB_AT	369.167 <sup>a</sup>	1	369.167	37.360	<.001	.053	37.360	1.000
	LDB_BI	1943.188 <sup>b</sup>	1	1943.188	99.266	<.001	.130	99.266	1.000
Intercept	LDB_AT	342230.843	1	342230.843	34633.964	.000	.981	34633.964	1.000
	LDB_BI	171191.822	1	171191.822	8745.208	.000	.929	8745.208	1.000
LDB_PE	LDB_AT	369.167	1	369.167	37.360	<.001	.053	37.360	1.000
	LDB_BI	1943.188	1	1943.188	99.266	<.001	.130	99.266	1.000
Error	LDB_AT	6580.989	666	9.881					
	LDB_BI	13037.284	666	19.576					
Total	LDB_AT	350456.000	668						
	LDB_BI	184233.000	668						
Corrected Total	LDB_AT	6950.156	667						
	LDB_BI	14980.472	667						

a. R Squared = .053 (Adjusted R Squared = .052) b. R Squared = .130 (Adjusted R Squared = .128) c. Computed using alpha = .05

Multivariate Tests<sup>a</sup>

Effect		Value	F	Hypothesis		Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power <sup>c</sup>
				df	Error df				
Intercept	Pillai's Trace	.980	15748.086 <sup>b</sup>	2.000	656.000	.000	.980	31496.172	1.000
	Wilks' Lambda	.020	15748.086 <sup>b</sup>	2.000	656.000	.000	.980	31496.172	1.000
	Hotelling's Trace	48.012	15748.086 <sup>b</sup>	2.000	656.000	.000	.980	31496.172	1.000
	Roy's Largest Root	48.012	15748.086 <sup>b</sup>	2.000	656.000	.000	.980	31496.172	1.000
LDB_EE	Pillai's Trace	.043	14.736 <sup>b</sup>	2.000	656.000	<.001	.043	29.473	.999
	Wilks' Lambda	.957	14.736 <sup>b</sup>	2.000	656.000	<.001	.043	29.473	.999
	Hotelling's Trace	.045	14.736 <sup>b</sup>	2.000	656.000	<.001	.043	29.473	.999
	Roy's Largest Root	.045	14.736 <sup>b</sup>	2.000	656.000	<.001	.043	29.473	.999

a. Design: Intercept + LDB\_EE b. Exact statistic c. Computed using alpha = .05

## Tests of Between-Subjects Effects

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared	Noncent. Paramete r	Observed Power <sup>c</sup>
Correcte d Model	LDB_AT	282.636 <sup>a</sup>	1	282.636	27.587	<.001	.040	27.587	.999
	LDB_BI	338.360 <sup>b</sup>	1	338.360	15.315	<.001	.023	15.315	.974
Intercept	LDB_AT	322425.143	1	322425.143	31470.974	.000	.980	31470.97 4	1.000
	LDB_BI	158680.946	1	158680.946	7182.289	.000	.916	7182.289	1.000
LDB_EE	LDB_AT	282.636	1	282.636	27.587	<.001	.040	27.587	.999
	LDB_BI	338.360	1	338.360	15.315	<.001	.023	15.315	.974
Error	LDB_AT	6731.070	657	10.245					
	LDB_BI	14515.342	657	22.093					
Total	LDB_AT	346667.000	659						
	LDB_BI	183110.000	659						
Correcte d Total	LDB_AT	7013.706	658						
	LDB_BI	14853.703	658						

a. R Squared = .040 (Adjusted R Squared = .039) b. R Squared = .023 (Adjusted R Squared = .021) c. Computed using alpha = .05

## Appendix J. Multivariate Tests Results (MANCOVA)

Multivariate Tests <sup>a</sup>									
Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power <sup>c</sup>
Intercept	Pillai's Trace	.965	7290.476 <sup>b</sup>	2.000	530.000	.000	.965	14580.952	1.000
	Wilks' Lambda	.035	7290.476 <sup>b</sup>	2.000	530.000	.000	.965	14580.952	1.000
	Hotelling's Trace	27.511	7290.476 <sup>b</sup>	2.000	530.000	.000	.965	14580.952	1.000
	Roy's Largest Root	27.511	7290.476 <sup>b</sup>	2.000	530.000	.000	.965	14580.952	1.000
PROC_TR	Pillai's Trace	.079	22.879 <sup>b</sup>	2.000	530.000	<.001	.079	45.759	1.000
	Wilks' Lambda	.921	22.879 <sup>b</sup>	2.000	530.000	<.001	.079	45.759	1.000
	Hotelling's Trace	.086	22.879 <sup>b</sup>	2.000	530.000	<.001	.079	45.759	1.000
	Roy's Largest Root	.086	22.879 <sup>b</sup>	2.000	530.000	<.001	.079	45.759	1.000
PROC_PC	Pillai's Trace	.107	31.735 <sup>b</sup>	2.000	530.000	<.001	.107	63.469	1.000
	Wilks' Lambda	.893	31.735 <sup>b</sup>	2.000	530.000	<.001	.107	63.469	1.000
	Hotelling's Trace	.120	31.735 <sup>b</sup>	2.000	530.000	<.001	.107	63.469	1.000
	Roy's Largest Root	.120	31.735 <sup>b</sup>	2.000	530.000	<.001	.107	63.469	1.000

a. Design: Intercept + PROC\_TR + PROC\_PC b. Exact statistic c. Computed using alpha = .05

### Tests of Between-Subjects Effects

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power <sup>c</sup>
Corrected Model	Proc_AT	706.388 <sup>a</sup>	2	353.194	39.195	<.001	.129	78.390	1.000
	Proc_BI	1601.835 <sup>b</sup>	2	800.918	45.748	<.001	.147	91.496	1.000
Intercept	Proc_AT	130469.144	1	130469.144	14478.604	.000	.965	14478.604	1.000
	Proc_BI	70780.648	1	70780.648	4042.955	<.001	.884	4042.955	1.000
PROC_TR	Proc_AT	315.627	1	315.627	35.026	<.001	.062	35.026	1.000
	Proc_BI	543.740	1	543.740	31.058	<.001	.055	31.058	1.000
PROC_PC	Proc_AT	335.053	1	335.053	37.182	<.001	.065	37.182	1.000
	Proc_BI	935.584	1	935.584	53.440	<.001	.091	53.440	1.000
Error	Proc_AT	4784.930	531	9.011					
	Proc_BI	9296.300	531	17.507					
Total	Proc_AT	290282.000	534						
	Proc_BI	173492.000	534						
Corrected Total	Proc_AT	5491.318	533						
	Proc_BI	10898.135	533						

a. R Squared = .129 (Adjusted R Squared = .125) b. R Squared = .147 (Adjusted R Squared = .144) c. Computed using alpha = .05



Multivariate Tests <sup>a</sup>									
Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power <sup>c</sup>
Intercept	Pillai's Trace	.964	5075.865 <sup>b</sup>	2.000	384.000	<.001	.964	10151.730	1.000
	Wilks' Lambda	.036	5075.865 <sup>b</sup>	2.000	384.000	<.001	.964	10151.730	1.000
	Hotelling's Trace	26.437	5075.865 <sup>b</sup>	2.000	384.000	<.001	.964	10151.730	1.000
	Roy's Largest Root	26.437	5075.865 <sup>b</sup>	2.000	384.000	<.001	.964	10151.730	1.000
WCM_TR	Pillai's Trace	.064	13.046 <sup>b</sup>	2.000	384.000	<.001	.064	26.091	.997
	Wilks' Lambda	.936	13.046 <sup>b</sup>	2.000	384.000	<.001	.064	26.091	.997
	Hotelling's Trace	.068	13.046 <sup>b</sup>	2.000	384.000	<.001	.064	26.091	.997
	Roy's Largest Root	.068	13.046 <sup>b</sup>	2.000	384.000	<.001	.064	26.091	.997
WCM_PC	Pillai's Trace	.259	67.105 <sup>b</sup>	2.000	384.000	<.001	.259	134.211	1.000
	Wilks' Lambda	.741	67.105 <sup>b</sup>	2.000	384.000	<.001	.259	134.211	1.000
	Hotelling's Trace	.350	67.105 <sup>b</sup>	2.000	384.000	<.001	.259	134.211	1.000
	Roy's Largest Root	.350	67.105 <sup>b</sup>	2.000	384.000	<.001	.259	134.211	1.000

a. Design: Intercept + WCM\_TR + WCM\_PC b. Exact statistic c. Computed using alpha = .05

Tests of Between-Subjects Effects									
Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power <sup>c</sup>
Corrected Model	WCM_AT	401.097 <sup>a</sup>	2	200.548	20.848	<.001	.098	41.695	1.000
	WCM_BI	2302.348 <sup>b</sup>	2	1151.174	77.358	<.001	.287	154.717	1.000
Intercept	WCM_AT	95946.091	1	95946.091	9973.920	<.001	.963	9973.920	1.000
	WCM_BI	54695.736	1	54695.736	3675.527	<.001	.905	3675.527	1.000
WCM_TR	WCM_AT	171.172	1	171.172	17.794	<.001	.044	17.794	.988
	WCM_BI	310.299	1	310.299	20.852	<.001	.051	20.852	.995
WCM_PC	WCM_AT	230.263	1	230.263	23.937	<.001	.059	23.937	.998
	WCM_BI	1993.387	1	1993.387	133.955	<.001	.258	133.955	1.000
Error	WCM_AT	3703.583	385	9.620					
	WCM_BI	5729.209	385	14.881					
Total	WCM_AT	216970.000	388						
	WCM_BI	135550.000	388						
Corrected Total	WCM_AT	4104.680	387						
	WCM_BI	8031.557	387						

a. R Squared = .098 (Adjusted R Squared = .093) b. R Squared = .287 (Adjusted R Squared = .283) c. Computed using alpha = .05

Multivariate Tests<sup>a</sup>

Effect		Value	F	Hypothesis		Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power <sup>c</sup>
				df	Error df				
Intercept	Pillai's Trace	.958	7409.210 <sup>b</sup>	2.000	645.000	.000	.958	14818.420	1.000
	Wilks' Lambda	.042	7409.210 <sup>b</sup>	2.000	645.000	.000	.958	14818.420	1.000
	Hotelling's Trace	22.974	7409.210 <sup>b</sup>	2.000	645.000	.000	.958	14818.420	1.000
	Roy's Largest Root	22.974	7409.210 <sup>b</sup>	2.000	645.000	.000	.958	14818.420	1.000
LDB_TR	Pillai's Trace	.048	16.179 <sup>b</sup>	2.000	645.000	<.001	.048	32.358	1.000
	Wilks' Lambda	.952	16.179 <sup>b</sup>	2.000	645.000	<.001	.048	32.358	1.000
	Hotelling's Trace	.050	16.179 <sup>b</sup>	2.000	645.000	<.001	.048	32.358	1.000
	Roy's Largest Root	.050	16.179 <sup>b</sup>	2.000	645.000	<.001	.048	32.358	1.000
LDB_PC	Pillai's Trace	.145	54.523 <sup>b</sup>	2.000	645.000	<.001	.145	109.045	1.000
	Wilks' Lambda	.855	54.523 <sup>b</sup>	2.000	645.000	<.001	.145	109.045	1.000
	Hotelling's Trace	.169	54.523 <sup>b</sup>	2.000	645.000	<.001	.145	109.045	1.000
	Roy's Largest Root	.169	54.523 <sup>b</sup>	2.000	645.000	<.001	.145	109.045	1.000

## Tests of Between-Subjects Effects

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared	Noncent. Parameter	Observed Power <sup>c</sup>
Corrected Model	LDB_AT	598.456 <sup>a</sup>	2	299.228	30.495	<.001	.086	60.990	1.000
	LDB_BI	2568.870 <sup>b</sup>	2	1284.435	67.505	<.001	.173	135.011	1.000
Intercept	LDB_AT	145592.908	1	145592.908	14837.803	.000	.958	14837.803	1.000
	LDB_BI	67894.658	1	67894.658	3568.304	<.001	.847	3568.304	1.000
LDB_TR	LDB_AT	229.252	1	229.252	23.364	<.001	.035	23.364	.998
	LDB_BI	465.819	1	465.819	24.482	<.001	.037	24.482	.999
LDB_PC	LDB_AT	353.990	1	353.990	36.076	<.001	.053	36.076	1.000
	LDB_BI	2050.506	1	2050.506	107.767	<.001	.143	107.767	1.000
Error	LDB_AT	6338.743	646	9.812					
	LDB_BI	12291.540	646	19.027					
Total	LDB_AT	341483.000	649						
	LDB_BI	179695.000	649						
Corrected Total	LDB_AT	6937.199	648						
	LDB_BI	14860.410	648						

a. R Squared = .086 (Adjusted R Squared = .083) b. R Squared = .173 (Adjusted R Squared = .170) c. Computed using alpha = .05

**Appendix K. Process Procedure Macro (Moderated Mediation Analysis)**

**Matrix**

Run MATRIX procedure:

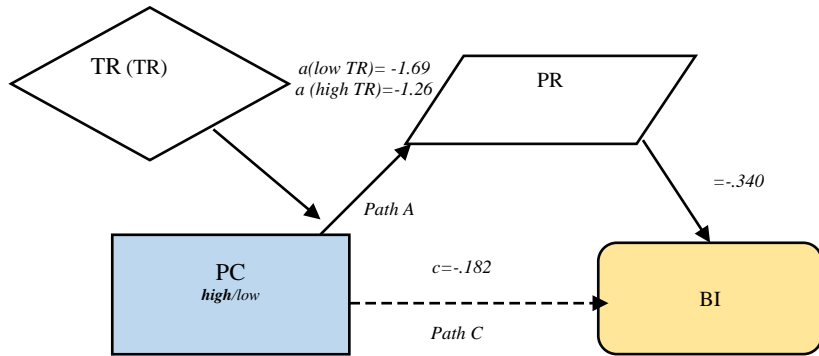
\*\*\*\*\* PROCESS Procedure for SPSS Version 4.2 \*\*\*\*\*

Written by Andrew F. Hayes, Ph.D. www.afhayes.com  
 Documentation available in Hayes (2022). www.guilford.com/p/hayes3

\*\*\*\*\*

Model : 7  
 Y : Proc\_AT  
 X : PROC\_PC  
 M : Proc\_PR  
 W : PROC\_TR

Sample Size: 530



\*\*\*\*\*

OUTCOME VARIABLE:

Proc\_PR

Model Summary

	R	R-sq	MSE	F	df1	df2
p	.603	.363	9.804	99.998	3.000	526.000
.000						

Model

	coeff	se	t	p	LLCI	ULCI
constant	7.746	.288	26.872	.000	7.180	8.312
PROC_PC	4.999	.391	12.796	.000	4.231	5.766
PROC_TR	-.746	.388	-1.924	.055	-1.507	.016
Int_1	-1.287	.546	-2.357	.019	-2.360	-.214

Product terms key:

Int\_1 : PROC\_PC x PROC\_TR

Test(s) of highest order unconditional interaction(s):

	R2-chng	F	df1	df2	p
X*W	.007	5.554	1.000	526.000	.019

-----

Focal predict: PROC\_PC (X)  
 Mod var: PROC\_TR (W)

Conditional effects of the focal predictor at values of the moderator(s):

PROC_TR	Effect	se	t	p	LLCI	ULCI
---------	--------	----	---	---	------	------

```

.000      4.999      .391      12.796      .000      4.231
5.766
1.000      3.712      .382      9.729      .000      2.962
4.462

```

Data for visualizing the conditional effect of the focal predictor:  
 Paste text below into a SPSS syntax window and execute to produce plot.

```

DATA LIST FREE/
  PROC_PC   PROC_TR   Proc_PR   .
BEGIN DATA.
  .000      .000      7.746
  1.000      .000      12.745
  .000      1.000      7.000
  1.000      1.000      10.712
END DATA.
GRAPH/SCATTERPLOT=
  PROC_PC WITH   Proc_PR BY   PROC_TR .

```

\*\*\*\*\*

OUTCOME VARIABLE:

Proc\_AT

Model Summary

	R	R-sq	MSE	F	df1	df2
p	.431	.186	8.408	60.133	2.000	527.000
	.000					

Model

	coeff	se	t	p	LLCI	ULCI
constant	26.471	.338	78.211	.000	25.806	27.136
PROC_PC	-.182	.307	-.594	.553	-.784	.420
Proc_PR	-.340	.039	-8.659	.000	-.417	-.263

\*\*\*\*\* DIRECT AND INDIRECT EFFECTS OF X ON Y \*\*\*\*\*

Direct effect of X on Y

Effect	se	t	p	LLCI	ULCI
-.182	.307	-.594	.553	-.784	.420

Conditional indirect effects of X on Y:

INDIRECT EFFECT:

PROC\_PC -> Proc\_PR -> Proc\_AT

PROC_TR	Effect	BootSE	BootLLCI	BootULCI
.000	-1.697	.237	-2.181	-1.254
1.000	-1.260	.200	-1.679	-.899

Index of moderated mediation (difference between conditional indirect effects):

	Index	BootSE	BootLLCI	BootULCI
PROC_TR	.437	.192	.082	.826

Pairwise contrasts between conditional indirect effects (Effect1 minus

```
Effect2)
  Effect1    Effect2    Contrast    BootSE    BootLLCI    BootULCI
    -1.260     -1.697         .437         .192         .082         .826
```

```
***** ANALYSIS NOTES AND ERRORS *****
```

```
Level of confidence for all confidence intervals in output:
```

```
95.0000
```

```
Number of bootstrap samples for percentile bootstrap confidence intervals:
```

```
5000
```

```
----- END MATRIX -----
```

**Matrix**

Run MATRIX procedure:

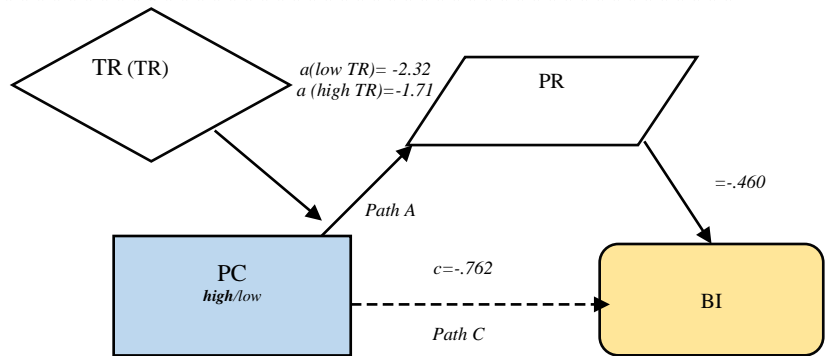
\*\*\*\*\* PROCESS Procedure for SPSS Version 4.2 \*\*\*\*\*

Written by Andrew F. Hayes, Ph.D. www.afhayes.com  
 Documentation available in Hayes (2022). www.guilford.com/p/hayes3

\*\*\*\*\*

Model : 7  
 Y : Proc\_BI  
 X : PROC\_PC  
 M : Proc\_PR  
 W : PROC\_TR

Sample Size: 531



\*\*\*\*\*

OUTCOME VARIABLE:

Proc\_PR

Model Summary

	R	R-sq	MSE	F	df1	df2
p	.605	.366	9.780	101.353	3.000	527.000
	.000					

Model

	coeff	se	t	p	LLCI	ULCI
constant	7.723	.287	26.939	.000	7.160	8.286
PROC_PC	5.045	.389	12.981	.000	4.281	5.808
PROC_TR	-.716	.387	-1.850	.065	-1.476	.044
Int_1	-1.340	.545	-2.460	.014	-2.410	-.270

Product terms key:

Int\_1 : PROC\_PC x PROC\_TR

Test(s) of highest order unconditional interaction(s):

	R2-chng	F	df1	df2	p
X*W	.007	6.050	1.000	527.000	.014

-----

Focal predict: PROC\_PC (X)  
 Mod var: PROC\_TR (W)

Conditional effects of the focal predictor at values of the moderator(s):

PROC_TR	Effect	se	t	p	LLCI	ULCI
---------	--------	----	---	---	------	------

```

.000      5.045      .389      12.981      .000      4.281
5.808
1.000      3.705      .382      9.707      .000      2.955
4.455

```

Data for visualizing the conditional effect of the focal predictor:  
 Paste text below into a SPSS syntax window and execute to produce plot.

```

DATA LIST FREE/
  PROC_PC   PROC_TR   Proc_PR   .
BEGIN DATA.
  .000      .000      7.723
  1.000      .000      12.768
  .000      1.000      7.007
  1.000      1.000      10.712
END DATA.
GRAPH/SCATTERPLOT=
  PROC_PC WITH   Proc_PR BY   PROC_TR .

```

\*\*\*\*\*

OUTCOME VARIABLE:

Proc\_BI

Model Summary

	R	R-sq	MSE	F	df1	df2
p	.453	.205	16.268	68.138	2.000	528.000
	.000					

Model

	coeff	se	t	p	LLCI	ULCI
constant	22.284	.471	47.353	.000	21.359	23.208
PROC_PC	-.762	.427	-1.786	.075	-1.601	.076
Proc_PR	-.460	.055	-8.441	.000	-.568	-.353

\*\*\*\*\* DIRECT AND INDIRECT EFFECTS OF X ON Y \*\*\*\*\*

Direct effect of X on Y

Effect	se	t	p	LLCI	ULCI
-.762	.427	-1.786	.075	-1.601	.076

Conditional indirect effects of X on Y:

INDIRECT EFFECT:

PROC\_PC -> Proc\_PR -> Proc\_BI

PROC_TR	Effect	BootSE	BootLLCI	BootULCI
.000	-2.323	.317	-2.944	-1.724
1.000	-1.706	.282	-2.279	-1.185

Index of moderated mediation (difference between conditional indirect effects):

	Index	BootSE	BootLLCI	BootULCI
PROC_TR	.617	.255	.125	1.127

Pairwise contrasts between conditional indirect effects (Effect1 minus

```
Effect2)
  Effect1    Effect2    Contrast    BootSE    BootLLCI    BootULCI
    -1.706     -2.323         .617         .255         .125         1.127
```

```
***** ANALYSIS NOTES AND ERRORS *****
```

```
Level of confidence for all confidence intervals in output:
```

```
95.0000
```

```
Number of bootstrap samples for percentile bootstrap confidence intervals:
```

```
5000
```

```
----- END MATRIX -----
```



**Matrix**

Run MATRIX procedure:

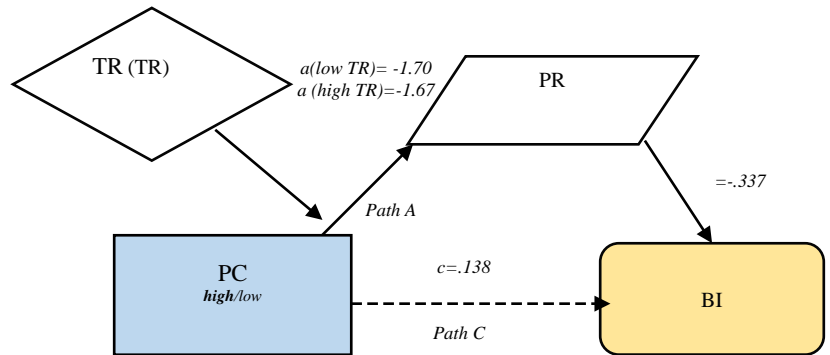
\*\*\*\*\* PROCESS Procedure for SPSS Version 4.2 \*\*\*\*\*

Written by Andrew F. Hayes, Ph.D. www.afhayes.com  
 Documentation available in Hayes (2022). www.guilford.com/p/hayes3

\*\*\*\*\*

Model : 7  
 Y : WCM\_AT  
 X : WCM\_PC  
 M : WCM\_PR  
 W : WCM\_TR

Sample Size: 386



\*\*\*\*\*

OUTCOME VARIABLE:  
 WCM\_PR

Model Summary

	R	R-sq	MSE	F	df1	df2
p	.633	.400	9.702	85.033	3.000	382.000
	.000					

Model

	coeff	se	t	p	LLCI	ULCI
constant	6.777	.321	21.093	.000	6.145	7.408
WCM_PC	5.046	.459	10.984	.000	4.142	5.949
WCM_TR	-.738	.444	-1.660	.098	-1.611	.136
Int_1	-.074	.635	-.117	.907	-1.323	1.174

Product terms key:

Int\_1 : WCM\_PC x WCM\_TR

Test(s) of highest order unconditional interaction(s):

	R2-chng	F	df1	df2	p
X*W	.000	.014	1.000	382.000	.907

-----  
 Focal predict: WCM\_PC (X)  
 Mod var: WCM\_TR (W)

Conditional effects of the focal predictor at values of the moderator(s):

WCM_TR	Effect	se	t	p	LLCI	ULCI
--------	--------	----	---	---	------	------

```

.000      5.046      .459      10.984      .000      4.142
5.949
1.000      4.971      .438      11.339      .000      4.109
5.833

```

Data for visualizing the conditional effect of the focal predictor:  
 Paste text below into a SPSS syntax window and execute to produce plot.

```

DATA LIST FREE/
  WCM_PC      WCM_TR      WCM_PR      .
BEGIN DATA.
  .000      .000      6.777
  1.000      .000      11.822
  .000      1.000      6.039
  1.000      1.000      11.010
END DATA.
GRAPH/SCATTERPLOT=
  WCM_PC      WITH      WCM_PR      BY      WCM_TR      .

```

\*\*\*\*\*

OUTCOME VARIABLE:

WCM\_AT

Model Summary

	R	R-sq	MSE	F	df1	df2
p	.401	.161	8.960	36.685	2.000	383.000
	.000					

Model

	coeff	se	t	p	LLCI	ULCI
constant	26.349	.378	69.751	.000	25.606	27.092
WCM_PC	.138	.391	.353	.724	-.630	.906
WCM_PR	-.337	.049	-6.899	.000	-.433	-.241

\*\*\*\*\* DIRECT AND INDIRECT EFFECTS OF X ON Y \*\*\*\*\*

Direct effect of X on Y

Effect	se	t	p	LLCI	ULCI
.138	.391	.353	.724	-.630	.906

Conditional indirect effects of X on Y:

INDIRECT EFFECT:

WCM\_PC -> WCM\_PR -> WCM\_AT

WCM_TR	Effect	BootSE	BootLLCI	BootULCI
.000	-1.698	.324	-2.386	-1.107
1.000	-1.673	.313	-2.323	-1.097

Index of moderated mediation (difference between conditional indirect effects):

	Index	BootSE	BootLLCI	BootULCI
WCM_TR	.025	.220	-.407	.461

Pairwise contrasts between conditional indirect effects (Effect1 minus

```
Effect2)
  Effect1    Effect2    Contrast    BootSE    BootLLCI    BootULCI
    -1.673     -1.698         .025         .220         -.407         .461
```

```
***** ANALYSIS NOTES AND ERRORS *****
```

```
Level of confidence for all confidence intervals in output:
```

```
95.0000
```

```
Number of bootstrap samples for percentile bootstrap confidence intervals:
```

```
5000
```

```
----- END MATRIX -----
```

**Matrix**

Run MATRIX procedure:

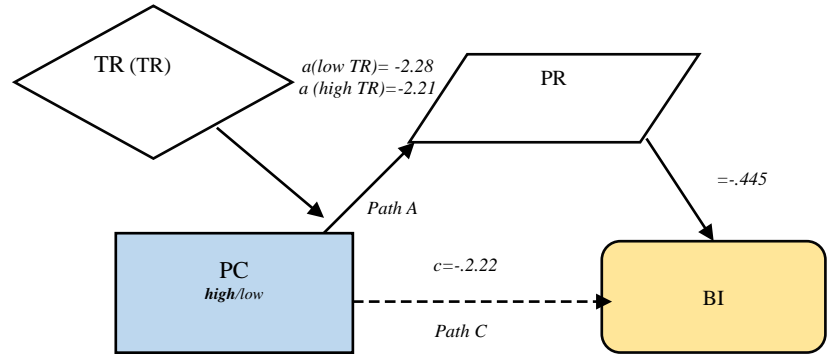
\*\*\*\*\* PROCESS Procedure for SPSS Version 4.2 \*\*\*\*\*

Written by Andrew F. Hayes, Ph.D. [www.afhayes.com](http://www.afhayes.com)  
 Documentation available in Hayes (2022). [www.guilford.com/p/hayes3](http://www.guilford.com/p/hayes3)

\*\*\*\*\*

Model : 7  
 Y : WCM\_BI  
 X : WCM\_PC  
 M : WCM\_PR  
 W : WCM\_TR

Sample Size: 395



\*\*\*\*\*

OUTCOME VARIABLE:  
 WCM\_PR

Model Summary

	R	R-sq	MSE	F	df1	df2
p	.639	.408	9.542	89.713	3.000	391.000
	.000					

Model

	coeff	se	t	p	LLCI	ULCI
constant	6.773	.314	21.595	.000	6.157	7.390
WCM_PC	5.117	.451	11.351	.000	4.231	6.003
WCM_TR	-.754	.435	-1.734	.084	-1.609	.101
Int_1	-.146	.623	-.234	.815	-1.370	1.078

Product terms key:

Int\_1 : WCM\_PC x WCM\_TR

Test(s) of highest order unconditional interaction(s):

	R2-chng	F	df1	df2	p
X*W	.000	.055	1.000	391.000	.815

-----

Focal predict: WCM\_PC (X)  
 Mod var: WCM\_TR (W)

Conditional effects of the focal predictor at values of the moderator(s):

WCM_TR	Effect	se	t	p	LLCI
--------	--------	----	---	---	------

```

ULCI
      .000      5.117      .451      11.351      .000      4.231
6.003
      1.000      4.971      .429      11.576      .000      4.127
5.815
  
```

Data for visualizing the conditional effect of the focal predictor:  
 Paste text below into a SPSS syntax window and execute to produce plot.

```

DATA LIST FREE/
  WCM_PC      WCM_TR      WCM_PR      .
BEGIN DATA.
      .000      .000      6.773
      1.000      .000      11.890
      .000      1.000      6.019
      1.000      1.000      10.990
END DATA.
GRAPH/SCATTERPLOT=
  WCM_PC      WITH      WCM_PR      BY      WCM_TR      .
  
```

```

*****
OUTCOME VARIABLE:
  WCM_BI
  
```

Model Summary

	R	R-sq	MSE	F	df1	df2
P	.575	.331	13.987	96.965	2.000	392.000
	.000					

Model

	coeff	se	t	p	LLCI	ULCI
constant	23.156	.468	49.461	.000	22.236	24.077
WCM_PC	-2.217	.485	-4.573	.000	-3.170	-1.264
WCM_PR	-.445	.061	-7.333	.000	-.564	-.326

\*\*\*\*\* DIRECT AND INDIRECT EFFECTS OF X ON Y \*\*\*\*\*

Direct effect of X on Y

Effect	se	t	p	LLCI	ULCI
-2.217	.485	-4.573	.000	-3.170	-1.264

Conditional indirect effects of X on Y:

INDIRECT EFFECT:

WCM_PC	->	WCM_PR	->	WCM_BI
WCM_TR	Effect	BootSE	BootLLCI	BootULCI
.000	-2.277	.402	-3.091	-1.521
1.000	-2.212	.442	-3.110	-1.400

Index of moderated mediation (difference between conditional indirect effects):

	Index	BootSE	BootLLCI	BootULCI
WCM_TR	.065	.278	-.531	.572

Pairwise contrasts between conditional indirect effects (Effect1 minus Effect2)

Effect1	Effect2	Contrast	BootSE	BootLLCI	BootULCI
-2.212	-2.277	.065	.278	-.531	.572

\*\*\*\*\* ANALYSIS NOTES AND ERRORS \*\*\*\*\*

Level of confidence for all confidence intervals in output:  
95.0000

Number of bootstrap samples for percentile bootstrap confidence intervals:  
5000

----- END MATRIX -----

**Matrix**

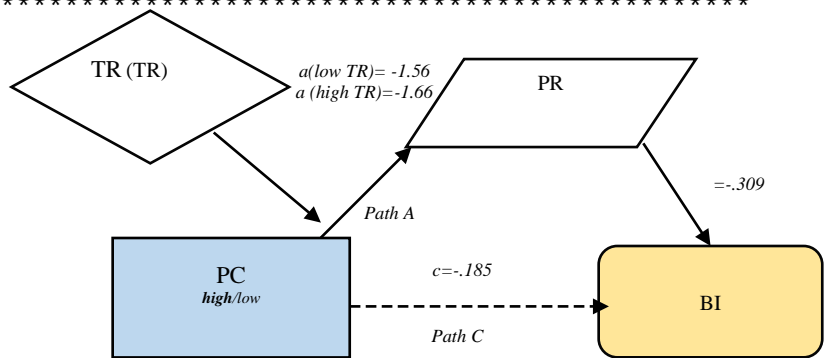
Run MATRIX procedure:

\*\*\*\*\* PROCESS Procedure for SPSS Version 4.2 \*\*\*\*\*

Written by Andrew F. Hayes, Ph.D. [www.afhayes.com](http://www.afhayes.com)  
 Documentation available in Hayes (2022). [www.guilford.com/p/hayes3](http://www.guilford.com/p/hayes3)  
 \*\*\*\*\*

Model : 7  
 Y : LDB\_AT  
 X : LDB\_PC  
 M : LDB\_PR  
 W : LDB\_TR

Sample Size: 646



\*\*\*\*\*

OUTCOME VARIABLE:  
 LDB\_PR

Model Summary

	R	R-sq	MSE	F	df1	df2
p	.614	.377	11.971	129.618	3.000	642.000
	.000					

Model

	coeff	se	t	p	LLCI	ULCI
constant	9.058	.293	30.864	.000	8.481	9.634
LDB_PC	5.044	.403	12.518	.000	4.253	5.836
LDB_TR	-1.280	.393	-3.257	.001	-2.052	-.508
Int_1	.321	.547	.588	.557	-.753	1.395

Product terms key:

Int\_1 : LDB\_PC x LDB\_TR

Test(s) of highest order unconditional interaction(s):

	R2-chng	F	df1	df2	p
X*W	.000	.345	1.000	642.000	.557

-----

Focal predict: LDB\_PC (X)  
 Mod var: LDB\_TR (W)

Conditional effects of the focal predictor at values of the moderator(s):

	LDB_TR	Effect	se	t	p	LLCI
ULCI						
	.000	5.044	.403	12.518	.000	4.253
5.836						
	1.000	5.366	.370	14.506	.000	4.639
6.092						

Data for visualizing the conditional effect of the focal predictor:  
 Paste text below into a SPSS syntax window and execute to produce plot.

```
DATA LIST FREE/
  LDB_PC  LDB_TR  LDB_PR  .
BEGIN DATA.
  .000    .000    9.058
  1.000    .000    14.102
  .000    1.000    7.777
  1.000    1.000    13.143
END DATA.
GRAPH/SCATTERPLOT=
  LDB_PC  WITH  LDB_PR  BY  LDB_TR  .
*****
OUTCOME VARIABLE:
  LDB_AT
```

Model Summary

	R	R-sq	MSE	F	df1	df2
p	.401	.161	8.826	61.610	2.000	643.000
	.000					

Model

	coeff	se	t	p	LLCI	ULCI
constant	26.051	.326	80.013	.000	25.411	26.690
LDB_PC	.185	.293	.634	.527	-.389	.760
LDB_PR	-.309	.033	-9.241	.000	-.375	-.243

\*\*\*\*\* DIRECT AND INDIRECT EFFECTS OF X ON Y \*\*\*\*\*

Direct effect of X on Y

Effect	se	t	p	LLCI	ULCI
.185	.293	.634	.527	-.389	.760

Conditional indirect effects of X on Y:

INDIRECT EFFECT:

LDB_PC	->	LDB_PR	->	LDB_AT
LDB_TR	Effect	BootSE	BootLLCI	BootULCI
.000	-1.559	.220	-2.016	-1.145
1.000	-1.659	.228	-2.118	-1.223

Index of moderated mediation (difference between conditional indirect effects):



	Index	BootSE	BootLLCI	BootULCI
LDB_TR	-.099	.170	-.440	.227

Pairwise contrasts between conditional indirect effects (Effect1 minus Effect2)

Effect1	Effect2	Contrast	BootSE	BootLLCI	BootULCI
-1.659	-1.559	-.099	.170	-.440	.227

\*\*\*\*\* ANALYSIS NOTES AND ERRORS \*\*\*\*\*

Level of confidence for all confidence intervals in output:

95.0000

Number of bootstrap samples for percentile bootstrap confidence intervals:

5000

----- END MATRIX -----

**Matrix**

Run MATRIX procedure:

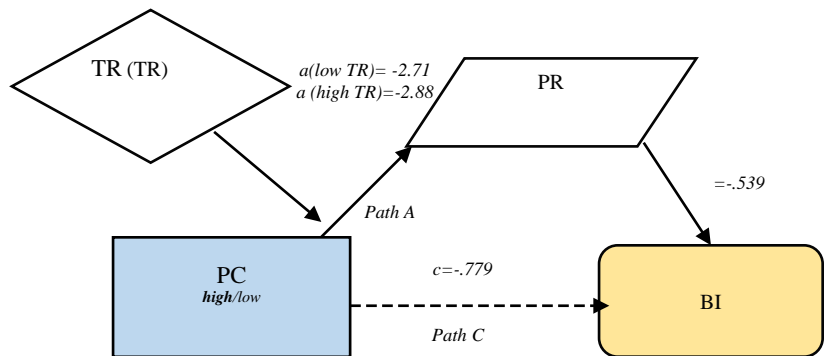
\*\*\*\*\* PROCESS Procedure for SPSS Version 4.2 \*\*\*\*\*

Written by Andrew F. Hayes, Ph.D. [www.afhayes.com](http://www.afhayes.com)  
 Documentation available in Hayes (2022). [www.guilford.com/p/hayes3](http://www.guilford.com/p/hayes3)

\*\*\*\*\*

Model : 7  
 Y : LDB\_BI  
 X : LDB\_PC  
 M : LDB\_PR  
 W : LDB\_TR

Sample Size: 648



\*\*\*\*\*

OUTCOME VARIABLE:  
 LDB\_PR

Model Summary

	R	R-sq	MSE	F	df1	df2
P	.612	.374	11.972	128.416	3.000	644.000
	.000					

Model

	coeff	se	t	p	LLCI	ULCI
constant	9.092	.291	31.202	.000	8.520	9.664
LDB_PC	5.036	.402	12.525	.000	4.246	5.826
LDB_TR	-1.271	.393	-3.239	.001	-2.042	-.501
Int_1	.300	.546	.550	.582	-.772	1.373

Product terms key:

Int\_1 : LDB\_PC x LDB\_TR

Test(s) of highest order unconditional interaction(s):

	R2-chng	F	df1	df2	p
X*W	.000	.303	1.000	644.000	.582

-----

Focal predict: LDB\_PC (X)  
 Mod var: LDB\_TR (W)

Conditional effects of the focal predictor at values of the moderator(s):

	LDB_TR	Effect	se	t	p	LLCI
ULCI						
	.000	5.036	.402	12.525	.000	4.246
5.826						
	1.000	5.336	.369	14.446	.000	4.611
6.062						

Data for visualizing the conditional effect of the focal predictor:  
 Paste text below into a SPSS syntax window and execute to produce plot.

```
DATA LIST FREE/
  LDB_PC      LDB_TR      LDB_PR      .
BEGIN DATA.
  .000        .000        9.092
  1.000        .000        14.128
  .000        1.000        7.821
  1.000        1.000        13.157
END DATA.
GRAPH/SCATTERPLOT=
  LDB_PC      WITH      LDB_PR      BY      LDB_TR      .
```

\*\*\*\*\*  
 OUTCOME VARIABLE:  
 LDB\_BI

Model Summary

	R	R-sq	MSE	F	df1	df2
P	.545	.297	16.087	136.344	2.000	645.000
	.000					

Model

	coeff	se	t	p	LLCI	ULCI
constant	22.303	.441	50.588	.000	21.437	23.169
LDB_PC	-.779	.393	-1.980	.048	-1.551	-.006
LDB_PR	-.539	.045	-11.954	.000	-.627	-.450

\*\*\*\*\* DIRECT AND INDIRECT EFFECTS OF X ON Y \*\*\*\*\*

Direct effect of X on Y

Effect	se	t	p	LLCI	ULCI
-.779	.393	-1.980	.048	-1.551	-.006

Conditional indirect effects of X on Y:

INDIRECT EFFECT:

LDB\_PC -> LDB\_PR -> LDB\_BI

LDB_TR	Effect	BootSE	BootLLCI	BootULCI
.000	-2.714	.330	-3.397	-2.108
1.000	-2.876	.358	-3.608	-2.232

Index of moderated mediation (difference between conditional indirect effects):

	Index	BootSE	BootLLCI	BootULCI
LDB_TR	-.162	.294	-.752	.387

Pairwise contrasts between conditional indirect effects (Effect1 minus Effect2)

Effect1	Effect2	Contrast	BootSE	BootLLCI	BootULCI
-2.876	-2.714	-.162	.294	-.752	.387

\*\*\*\*\* ANALYSIS NOTES AND ERRORS \*\*\*\*\*

Level of confidence for all confidence intervals in output:  
95.0000

Number of bootstrap samples for percentile bootstrap confidence intervals:  
5000

----- END MATRIX -----

## References

- Abdou, D., & Jasimuddin, S. M. (2020). The use of the UTAUT model in the adoption of e-learning technologies: An empirical study in France based banks. *Journal of Global Information Management*, 28(4), 38–51. <https://doi.org/10.4018/JGIM.2020100103>
- Aisyah, S., Bandung, Y., & Subekti, L. B. (2018). Development of continuous authentication system on android-based online exam application. *Proceedings of the International Conference on Information Technology Systems and Innovation (ICITSI)*, 171-176. <https://doi: 10.1109/ICITSI.2018.8695954>
- Alessio, H. M., Malay, N., Maurer, K., Bailer, A. J., & Rubin, B. (2017). Examining the effect of proctoring on online test scores, *Online Learning*, 21(1), 146-161. <https://doi.org/10.24059/olj.v21i1.885>
- Alkhateeb, J. H. (2020). A novel framework for ensuring online exam authentication at Taibah University. *International Journal of Software Engineering and Computer Systems*, 6(1), 1-7. <https://doi.org/10.15282/ijsecs.6.1.2020.1.0064>
- Almaiah, M. A., Al-Otaibi, S., Shishakly, R., Hassan, L., Lutfi, A., Alrawad, M., Qataweh, M., & Alghanam, O. A. (2023). Investigating the role of perceived risk, perceived security and perceived trust on Smart m-Banking Application using SEM Sustainability (Basel, Switzerland), 15(13), 1-17. <https://doi.org/10.3390/su15139908>
- Alowayr, A. (2021). Determinants of mobile learning adoption: Extending the unified theory of acceptance and use of technology (UTAUT). *The International Journal of Information and Learning Technology*, 39(1), 1–12. <https://doi.org/10.1108/IJILT-05-2021-0070>
- Amigud, A., Arnedo-Moreno, J., Daradoumis, T., & Guerrero-Roldan, A. E. (2017). Using learning analytics for preserving academic integrity. *International Review of Research in Open and Distributed Learning*, 18(5), 192–210. <https://doi.org/10.19173/irrodl.v18i5.3103>
- Amigud, A., Arnedo-Moreno, J., Daradoumis, T., & Guerrero-Roldan, A. E. (2018). An integrative review of security and integrity strategies in an academic environment: Current understanding and emerging perspectives. *Computers & Security*, 76, 50–70. <https://doi-org.ezproxy.fiu.edu/10.1016/j.cose.2018.02.021>
- Apampa, K. M., Wills, G., & Argles, D. (2009). Towards security goals in summative E-Assessment Security. *2009 International Conference for Internet Technology and Secured Transactions, (ICITST)*, 1–5. <https://doi.org/10.1109/ICITST.2009.5402505>

- Apampa, K. M., & Wills, G., & Argeles, D. (2010). User security issues in summative e-assessment security. *International Journal for Digital Society, 1*(2), 135-147. <http://dx.doi.org/10.20533/ijds.2040.2570.2010.0018>
- Apampa, K. M., Wills, G., & Argles, D. (2011). Towards a blob-based presence verification system in summative e-assessments. *International Journal of e-Assessment, 1*(1), 1-17.
- Brandon, D. M., Long, J. H., Loraas, T. M., Mueller-Phillips, J., & Vansant, B. (2014). Online instrument delivery and participant recruitment services: Emerging opportunities for behavioral accounting research. *Behavioral Research in Accounting, 26* (1), 1-23. <https://doi.org/10.2308/bria-50651>
- Bristol, T. (2017). Test and examination security technology. *Teaching and Learning in Nursing, 12*(4), 320-322. <https://doi.org/10.1016/j.teln.2017.06.009>
- Brown, V. (2018). Evaluating technology to prevent academic integrity violations in online environments. *Online Journal of Distance Learning Administration, 21*(1), 1-11. <https://ojdla.com/archive/spring211/brown211.pdf>
- Cakır, R., & Solak, E. (2015). Attitude of Turkish EFL learners towards e-learning through TAM Model. *Procedia - Social and Behavioral Sciences, 176*, 596–601. <https://doi.org/10.1016/j.sbspro.2015.01.515>
- Chiu, C. M., & Wang, E. T. (2008). Understanding Web-based learning continuance intention: The role of subjective task value. *Information & Management, 45*(3), 194–201. <https://doi.org/10.1016/j.im.2008.02.003>
- Chou, H. L., & Chen, C., H. (2016). Beyond identifying privacy issues in e-learning settings: Implications for instructional designers. *Computers & Education, 103*, 124–133. <https://doi.org/10.1016/j.compedu.2016.10.002>
- Cifuentes, L., & Janney, A. (2016). Protecting students' integrity and reducing academic dishonesty in online learning. *Distance Learning, 13*(4), 9-15. <https://doi.org/10.3389/feduc.2021.639814>
- Clement, L. M., & Bradley-Garcia, M. (2022). A step-by-step tutorial for performing a moderate mediation analysis using PROCESS. *The Quantitative Methods for Psychology, 18*(3), 258-271. <https://doi.org/10.20982/tqmp.18.3.p258>
- Coughlan, M., Cronin, P., & Ryan, F. (2009). Survey research: Process and limitations. *International Journal of Therapy and Rehabilitation, 16*(1), 9–15. <https://doi.org/10.12968/ijtr.2009.16.1.37935>
- Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches*. (5<sup>th</sup> ed.). Sage.

- Davis, F. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340.  
<https://doi.org/10.2307/249008>
- Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, 35(8), 982–1003. <https://doi.org/10.1287/mnsc.35.8.982>
- Dwivedi, Y. K., Rana, N. P., Jeyaraj, A., Clement, M., & Williams, M. D. (2017). Re-examining the Unified Theory of Acceptance and Use of Technology (UTAUT): Towards a revised theoretical model. *Information Systems Frontiers*, 21(3), 719–734.  
<https://doi.org/10.1007/s10796-017-9774-y>
- Edwards, C., Holmes, W., Whitelock, D., & Okada, A. (2018). Student trust in e-authentication. In *Proceedings of the Fifth Annual ACM Conference on Learning at Scale*, 1-4. <https://doi.org/10.1145/3231644.3231700>
- Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science and Information Technology*, 6, 323-337. <https://doi.org/10.28945/1062>
- Escobar-Rodríguez, T., & Carvajal-Trujillo, E. (2014). Online purchasing tickets for low-cost carriers: An application of the unified theory of acceptance and use of technology (UTAUT) model. *Tourism Management*, 43, 70–88.  
<https://doi.org/10.1016/j.tourman.2014.01.017>
- Fenu, G., Marras, M., & Boratto, L. (2018). A multi-biometric system for continuous student authentication in e-learning platforms. *Pattern Recognition Letters*, 113, 83-92.  
<https://doi-org.ezproxy.fiu.edu/10.1016/j.patrec.2017.03.027>
- Fishbein, M. (1963). An investigation of the relationships between beliefs about an object and the attitude toward that object. *Human Relations*, 16(3), 233–239.  
<https://doi.org/10.1177/001872676301600302>
- Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention, and behavior: An introduction to theory and research. *Contemporary Sociology*, 6(2) 244–245.  
<https://doi.org/10.2307/2065853>
- Fisher, E., McLeod, A. J., Savage, A., & Simkin, M. G. (2016). Ghostwriters in the cloud. *Journal of Accounting Education*, 34, 59–71.  
<https://doiorg.ezproxy.fiu.edu/10.1016/j.jaccedu.2015.11.001>
- Flior, E., & Kowalski, K. (2010). Continuous biometric user authentication in online examinations. *Proceedings of the Seventh International Conference on Information Technology: New Generations, Information Technology: New Generations (ITNG), 2010 Seventh International Conference On*, 488–492.

- French, A., Macedo, M., Poulsen, J., Waterson, T., & Yu, A. (2008). Multivariate analysis of variance (MANOVA).
- Gathuri, J. W., Luvanda, A., Matende, S., & Kamundi, S. (2014). Impersonation challenges associated with e-Assessment of university students. *Journal of Information Engineering and Applications*, 4, 60-68.
- Giannakos, M. N., & Vlamos, P. (2013). Educational webcasts' acceptance: Empirical examination and the role of experience: Educational webcasts' acceptance and the role of experience. *British Journal of Educational Technology*, 44(1), 125–143. <https://doi.org/10.1111/j.1467-8535.2011.01279.x>
- Goodhue, D. (1988). I/S attitudes: toward theoretical and definitional clarity. *The Data Base for Advances in Information Systems*, 19(3-4), 6–15. <https://doi.org/10.1145/65766.65768>
- Goodhue, D., Thompson, R.L. (1995). Task-technology fit and individual performance. *MIS Quarterly*, 19 (2), 213–236. <https://doi.org/10.2307/249689>
- Granic, A., & Marangunic, N. (2019). Technology acceptance model in educational context: A systematic literature review. *British Journal of Educational Technology*, 50(5), 2572–2593. <https://doi.org/10.1111/bjet.12864>
- Guerro-Roldán, A. E., Rodríguez-González, M. E., Karadeniz, A., Kocdar, S., Aleksieva, L., & Peytcheva-Forsyth, R. (2020). Students' Experiences on using an authentication and authorship checking system in e-Assessment. *University Journal of Education*, 35, 6-24. <https://doi.10.16986/HUJE.2020063670>
- Hayes, A. F. (2022). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*. Guilford publications.
- Hernández-Álvarez, L., de Fuentes, J. M., González-Manzano, L., & Hernández Encinas, L. (2020). Privacy-Preserving sensor-based continuous authentication and user profiling: A review. *Sensors (Basel, Switzerland)*, 21(1), 1–23. <https://doi.org/10.3390/s21010092>
- Hussein, Z. (2017). Leading to Intention: The role of attitude in relation to Technology Acceptance Model in e-learning. *Procedia Computer Science*, 105, 159–164. <https://doi.org/10.1016/j.procs.2017.01.196>
- Hylton, K., Levy, Y., & Dringus, L. P. (2016). Utilizing webcam-based proctoring to deter misconduct in online exams. *Computers & Education*, 92–93, 53–63. <https://doi.org/10.1016/j.compedu.2015.10.002>
- Im, I., Kim, Y., & Han, H. J. (2008). The effects of perceived risk and technology type on users' acceptance of technologies. *Information & Management*, 45(1), 1–9. <https://doi.org/10.1016/j.im.2007.03.005>



- Kang, B., & Kim H. (2015). A design of e-learning authentication system. *International Journal of Security Applications* 9(1), 45–50. <https://doi.org/10.14257/ijasia.2015.9.1.05>
- James, T., Pirim, T., Boswell, K., Reithel, B., & Barkhi, R. (2008). An extension of the technology acceptance model to determine the intention to use biometric devices. In Clarke, S., (Ed.), *End User Computing Challenges and Technologies: Emerging Tools and Applications* (pp. 57-78). IGI Global. <https://doi.org/10.4018/978-1-59904-295-4.ch005>
- Jungbok, H. (2016). Multivariate analysis of variance in marketing research. *Advances in Management*, 9(9), 1-5.
- Kanak, A., & Sogukpinar, I. (2017). BioTAM: A technology acceptance model for biometric authentication systems. *IET Biometrics*, 6(6), 457-467. <https://doi.org/10.1049/iet-bmt.2016.0148>
- Khalilzadeh, J., Ozturk, A. B., & Bilgihan, A. (2017). Security-related factors in extended UTAUT model for NFC based mobile payment in the restaurant industry. *Computers in Human Behavior*, 70, 460–474. <https://doi.org/10.1016/j.chb.2017.01.001>
- Kharbat, F. F., & Abu Daabes, A. S. (2021). E-proctored exams during the COVID-19 pandemic: A close understanding. *Education and Information Technologies*, 26(6), 6589–6605. <https://doi.org/10.1007/s10639-021-10458-7>
- Laamanen, M., Ladonlahti, T., Uotinen, S., Okada, A., Bañeres, D., & Koçdar, S. (2021). Acceptability of the e-authentication in higher education studies: Views of students with special educational needs and disabilities. *International Journal of Educational Technology in Higher Education*, 18(1), 1-17. <https://doi.org/10.1186/s41239-020-00236-9>
- Lavrakas, P. J. (2008). *Encyclopedia of survey research methods* (Vols. 1-0). Sage Publications Inc. <https://doi.org/10.4135/9781412963947>
- Leedy, P. D., & Ormrod, J. E. (2010). *Practical research: Planning and design* (9th ed.). Pearson Educational International.
- Lee-Post, A., Hapke, H. (2017). Online learning integrity approaches: Current practices and future solutions. *Online Learning*, 21(1), 135–145.
- Levy, Y., & Ramim, M. M. (2009). Initial development of a learners' ratified acceptance of multibiometric intentions model (RAMIM). *Interdisciplinary Journal of E-Learning & Learning Objects*, 5, 379–397. <https://doi.org/10.28945/84>
- Levy Y., Ramim M., Furnell S., & Clarke N. (2011). Comparing intentions to use university-provided vs vendor-provided multibiometric authentication in online exams. *Campus-Wide Information Systems*, 28(2), 102–113.

- Lilley, M., Meere, J., & Barker, T. (2016). Remote live invigilation: A pilot study. *Journal of Interactive Media in Education*, 2016(1), 1–5. <https://doi.org/10.5334/jime.408>
- Liu, C., Marchewka, J. T., Lu, J., & Yu, C. S. (2005). Beyond concern, a privacy-trust-behavioral intention model of electronic commerce. *Information & Management*, 42(2), 289–304. <https://doi.org/10.1016/j.im.2004.01.003>
- McCole, P., Ramsey, E., & Williams, J. (2010). Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns. *Journal of Business Research*, 63(9), 1018–1024. <https://doi.org/10.1016/j.jbusres.2009.02.025>
- Miltgen, C. L., Popovič, A., & Oliveira, T. (2013). Determinants of end-user acceptance of biometrics: Integrating the “Big 3” of technology acceptance with privacy context. *Decision Support Systems*, 56, 103–114. <https://doi.org/10.1016/j.dss.2013.05.010>
- Moini, A., & Madni, A. M. (2009). Leveraging biometrics for user authentication in online learning: A systems perspective. *IEEE Systems Journal*, 3(4), 469–476. <https://doi.org/10.1109/JSYST.2009.2038957>
- Moriuchi, E. (2021). An empirical study of consumers’ intention to use biometric facial recognition as a payment method. *Psychology & Marketing*, 38(10), 1741–1765. <https://doi.org/10.1002/mar.21495>
- Naveen J., Kumar, M. G., Mukhilan, P., Prasad, V. M., Ramasamy, T., & Harini, N. (2018). Multi-factor authentication scheme for online examination, *International Journal of Pure and Applied Mathematics*, 119, 1705-1712.
- Niinuma, K., Park, U., & Jain, A. K. (2010). Soft biometric traits for continuous user authentication. *IEEE Transactions on Information Forensics and Security*, 5(4), 771 -780. Doi: <https://doi.org/10.1109/TIFS.2010.2075927>
- Okada, A., Whitelock, D., Holmes, W., & Edwards, C. (2019). E-Authentication for online assessment: A mixed-method study. *British Journal of Educational Technology*, 50(2), 861-875. <https://doi.org/10.1111/bjet.12608>
- Oliveira, T., Faria, M., Thomas, M. A., & Popovič, A. (2014). Extending the understanding of mobile banking adoption: When UTAUT meets TTF and ITM. *International Journal of Information Management*, 34(5), 689–703. <https://doi.org/10.1016/j.ijinfomgt.2014.06.004>
- Peris-Lopez, P., González-Manzano, L., Camara, C., & de Fuentes, J. M. (2018). Effect of attacker characterization in ECG-based continuous authentication mechanisms for internet of things. *Future Generation Computer Systems*, 81, 67–77. <https://doi.org/10.1016/j.future.2017.11.037>

- Prakash, A., & Mukesh, R. (2014). A biometric approach for continuous user authentication by fusing hard and soft traits. *International Journal of Network Security*, 16, 65-70.
- Rahman, M. M., Lesch, M. F., Horrey, W. J., & Strawderman, L. (2017). Assessing the utility of TAM, TPB, and UTAUT for advanced driver assistance systems. *Accident Analysis and Prevention*, 108, 361–373. <https://doi.org/10.1016/j.aap.2017.09.011>
- Ryu, R., Yeom, S., Kim, S. H., & Herbert, D. (2021). Continuous multimodal biometric authentication schemes: A systematic review. *IEEE Access*, 9, 34541–34557. <https://doi.org/10.1109/ACCESS.2021.3061589>
- Sabbah, Y. W. (2017). Security of online examinations. In I. Palomares Carrascosa, H. Kalutarage, & Y. Huang (Eds.), *Data Analytics and Decision Support for Cybersecurity* (pp. 157-200). Springer. <https://doi.org/10.1007/978-3-319-59439-2>
- Salloum, S. A., Al-Emran, M., Shaalan, K., & Tarhini, A. (2019). Factors affecting the E-learning acceptance: A case study from UAE. *Education and Information Technologies*, 24(1), 509-530. <https://doi.org/10.1007/s10639-018-9786-3>
- Schaefer, T., Barta, M., & Pavone, T. (2009). Student identity verification and the higher education opportunity Act: A faculty perspective. *Instructor*, 59, 252. [https://www.itdl.org/Journal/Aug\\_09/article05.htm](https://www.itdl.org/Journal/Aug_09/article05.htm)
- Scott, J. E. (1995) The measurement of information systems effectiveness: Evaluating a measuring instrument. *SIGMIS Database* 26(1), 43–61. <https://doi.org/10.1145/206476.206484>
- Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill building approach*, (7<sup>th</sup> ed.). Wiley.
- Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. (2006) Concern for information privacy and online consumer purchasing, *Journal of the Association for Information Systems*, 7(6), 415-444. <https://doi.org/10.17705/1jais.00092>
- Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, 13(2),147–169. <https://doi.org/10.2307/248922>
- Straub, D. W., Bourdreau, M., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, 13(24), 380–427. <https://doi.org/10.17705/1CAIS.01324>
- Stephan, S. H. (2017). Trust-related privacy factors in e-learning environments. *Distance Learning*, 14(4), 49–54.
- Taherdoost, H. (2016). Validity and reliability of the research instrument; How to test the validation of a questionnaire/survey in research. *International Journal of Academic Research in Management (IJARM)*, 5(3), 28–36. <http://dx.doi.org/10.2139/ssrn.3205040>

- Tan, P. (2013). Applying the UTAUT to Understand Factors Affecting the Use of English E-Learning Websites in Taiwan. *SAGE Open*, 3(4), 1–12.  
<https://doi.org/10.1177/2158244013503837>
- Tarhini, A., El-Masri, M., Ali, M., & Serrano, A. (2016). Extending the UTAUT model to understand the customers' acceptance and use of internet banking in Lebanon: A structural equation modeling approach. *Information Technology & People*, 29(4), 830–849. <https://doi.org/10.1108/ITP-02-2014-0034>
- Ullah, A., Xiao, H., & Barker, T. (2016). A classification of threats to remote online examinations. In *Proceedings of the IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*. Vancouver, BC (pp. 1-7). [doi:10.1109/IEMCON.2016.7746085](https://doi.org/10.1109/IEMCON.2016.7746085)
- Ullah, A., Xiao, H., & Barker, T. (2018). A dynamic profile questions approach to mitigate impersonation in online examinations. *Journal of Grid Computing*, 2, 209–223. <https://doi-org.ezproxy.fiu.edu/10.1007/s10723-018-9442-6>
- Vallejo, G., Fernández, M. P., & Livacic-Rojas, P. E. (2023). Multivariate analysis of covariance for heterogeneous and incomplete data. *Psychological Methods*. Advance online publication. <https://doi.org/10.1037/met0000558>
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of Information Technology: Toward a unified view. *MIS Quarterly*, 27(3), 425–478. <https://doi.org/10.2307/30036540>
- Wang, Y.S., Wu, M. C., & Wang, H. Y. (2009). Investigating the determinants and age and gender differences in the acceptance of mobile learning. *British Journal of Educational Technology*, 40(1), 92–118. <https://doi.org/10.1111/j.14678535.2007.00809.x>
- Westen, D., & Rosenthal, R. (2003). Quantifying construct validity: Two simple measures *Journal of Personality and Social Psychology*, 84(3), 608–618. <https://doi.org/10.1037//0022-3514.84.3.608>
- Zhang, L., & Samaras, D. (2004). Pose invariant face Recognition under arbitrary unknown lighting using spherical harmonics. *Biometric Authentication*, 10–23. [https://doi.org/10.1007/978-3-540-25976-3\\_2](https://doi.org/10.1007/978-3-540-25976-3_2)
- Zhou, T. (2011). The impact of privacy concern on user adoption of location-based services. *Industrial Management & Data Systems*, 111(2), 212-226. <https://doi.org/10.1108/02635571111115146>