AUTHOEXAM: A BROWSER EXTENSION WITH MULTI-FACTOR AUTHENTICATION FOR PROCTORING ONLINE EXAMS

KATRINA ROMEI T. JIMENEA

SUBMITTED TO THE FACULTY OF THE INSTITUTE OF COMPUTER SCIENCE
UNIVERSITY OF THE PHILIPPINES LOS BAÑOS
IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE
DEGREE OF

BACHELOR OF SCIENCE IN COMPUTER SCIENCE

JUNE 2024

The Special Problem here attached entitled AUTHOEXAM: A BROWSER EXTENSION WITH MULTI-FACTOR AUTHENTICATION FOR PROCTORING ONLINE EXAMS, prepared and submitted by KATRINA ROMEI T. JIMENEA, in partial fulfillment of the requirements for the degree of BACHELOR OF SCIENCE IN COMPUTER SCIENCE is hereby accepted.

CONCEPCION L. KHAN
Adviser

____
Date Signed

DR. MARIA ART ANTONETTE D. CLARIÑO, PH.D.
Director, Institute Of Computer Science

____
Date Signed

The contents or any portion of this undergraduate thesis manuscript including the source code or any non-commercial section may be freely copied and distributed provided that the source is acknowledged. The following permission/s is/are granted for accessing this thesis:

Available to the general public	NO
Available only after consultation with author/thesis adviser	YES
Available only to those bound by confidentiality agreements	YES

KATRINA ROMEI T. JIMENEA
Author/Advisee

June 16, 2024
Date Signed

BIOGRAPHICAL SKETCH

Katrina Romei is a Computer Science student from the University of the Philippines Los Baños. She is interested in web development projects that benefit the community. She is a member of the Alliance of Computer Science Students UPLB.

KATRINA ROMEI T. JIMENEA

ACKNOWLEDGEMENT

First and foremost, I would like to express my gratitude to God for His divine guidance and blessing throughout this journey.

I am grateful to my family for their unwavering support and being my pillars of strength.

I would like to thank my adviser, Ma'am Khan, whose expertise and patience significantly guided me throughout the process of creating and developing my SP. I would also like to acknowledge the Institute of Computer Science for allowing my proctoring tool to be tested by some instructors.

To all my friends, who have been nothing but supportive of me while I was working on my SP. They have been my source of comfort during the challenging times of writing and developing my SP.

TABLE OF CONTENTS

ABSTRACT

Academic institutions use online learning platforms for blended learning. As a result, most examinations are taken online, making it challenging to ensure academic integrity. This study presents AuthoExam, a proctoring tool that verifies a student's digital identity using multi-factor authentication (MFA) with knowledge and risk-based factors. The Chrome Extension API was also used to monitor real-time student browser activity. As a proctoring tool, AuthoExam generated various proctoring reports that showed and summarized students' flagged browser activity during the online exam and their weighted risk score for risk-based authentication. Ten respondents who have experience taking or scheduling online exams assessed the proctoring tool's usability by answering the System Usability questionnaire. The average score was 91.75, which indicated that AuthoExam was has high usability.

INTRODUCTION

Background of the Study

Open and Distance e-learning (ODeL) is an online and flexible learning mode for learners who cannot attend traditional face-to-face classes. Numerous universities used this learning method throughout the COVID-19 pandemic. Students used Learning Management Systems to study and access course material to continue learning online. As cases of infection dropped in 2022, governments started to allow in-person gatherings. Therefore, educational institutions are adopting hybrid or blended learning, which combines on-site and online learning strategies. Measurements of extreme heat indexes in the Philippines led to another implementation of distance learning. In a memorandum to school administrators, the CALABARZON Department of Education (DepEd) head suggested switching to modular distance learning (Mallari Jr., 2024). Similarly, faculty members at the University of the Philippines were allowed to switch into remote or asynchronous classes (University of the Philippines Tacloban, 2024; Untalan, 2024). In situations where face-to-face classes are interrupted, the option to shift to online learning allows schools to provide students with more flexibility in how they learn. Course assessments in online education are posted on online learning management systems. For examinations, some use free online form builders like Google Forms. Despite the benefits of online learning, the remote nature of online assessments raised concerns. Confirming the student's identity is one of the most common issues, as ensuring that the right student is taking the exam can be challenging. Another concern is plagiarizing the assessments students submit online (Nurunnabi & Hossain, 2019) and hiring someone to take their exams. Moreover, students can also access other websites and share the exam questions online (Reedy et al., 2021). These issues compromise the integrity and fairness of online assessments. This is a form of academic dishonesty and must be addressed by educational institutions. Educational institutions have started using learning management systems with authentication tools like Google Auth ID (Nguyen, 2022), OpenID Connect (Sujanani & Vinod, 2018), and Single Sign-On services to address authenticating and verifying student's identity online.

However, because proctoring occurs remotely or not at all, monitoring student activity during online examinations is challenging. To help with this, learning management systems such as Canvas support web-based proctoring software tools like Respondus and Honorlock. These proctoring tools use machine learning algorithms to monitor and analyze student behavior during online assessments. To help with this, learning management systems such as Canvas support web-based proctoring software tools like Respondus and Honorlock. These proctoring tools use machine learning algorithms to monitor and analyze student behavior during online assessments. These tools can be effective in preventing academic dishonesty, but they can be expensive. There are also concerns regarding privacy and integrating the tool with institutional learning management systems. Additionally, there are concerns about the technical performance and reliability of proctoring systems due to slow internet bandwidth and poor hardware and reporting capabilities (Hussein et al., 2020). The developed proctoring tool in this paper is a browser extension that authenticates students' digital identities and monitors their browser activities during the assessment. To verify the student taking the assessment, the proctoring tool will gather data from the student, which includes attributes for their digital identity. The proctoring tool authenticates this data using multi-factor authentication and Weighted Risk Scoring. Additionally, the Browser Extension Application Programming Interface (API) will monitor student browser activity, including access to other websites, during the assessment to flag suspicious behavior.

Significance of the Study

The proctoring tool in this study aims to help academic institutions proctor online assessments and address possible cheating issues. As academic institutions have become more reliant on online learning platforms to facilitate learning, it is important to maintain and ensure the academic integrity of online assessments. The importance of the proctoring tool is to provide teachers with a proctoring tool that can be used with different learning management systems and can proctor different types of online assessments. The proctoring tool can provide information about the online identity and activity of the student while taking an online exam. Information such as browsing activity can monitor attempts of accessing external websites as well as using copy-paste. Additionally, the use of multi-factor authentication can enhance web authentication and reduce the risk of digital identity impersonation. This feature of the proctoring tool will verify that the online assessment is answered by the intended student and not by any unauthorized individual. Furthermore, this proctoring tool aids educational institutions and teachers to assure the integrity and credibility of online assessments as it measures the student's understanding of the subject matter.

Research Problem

There are tools available for monitoring and tracking student activity during online exams, these tools often come with a cost and are typically integrated with premium learning management systems. Moreover, most research and software developments have focused on the tab management features of browser extension APIs. This study aims to develop a proctoring tool browser extension that authenticates students through Multi-factor Authentication and monitors their browser activity during online assessments. In developing a proctoring tool, the study intends to address the following questions:

1. What technologies will be used in developing the proctoring tool?

2. What are the key features that a proctoring tool should have?

3. How can the usability of the proctoring application be ensured?

Objectives of the Study

The main objective of this study is to develop a proctoring tool that will help educational institutions monitor online assessments.The specific objectives of this proctoring tool are:

1. To implement the use of Multi-factor authentication in verifying the identity of the student taking the online assessment

2. To integrate the Browser Extension API to monitor student activity while taking the assessment to flag possible cheating

3. To evaluate the usability of the proctoring tool using the System Usability Scale

Scope and Limitations

The scope of this study is the development of a browsing extension with Multi-factor authentication for proctoring online assessments. This study will solely authenticate students' digital identity using Multi-factor Authentication factors such as Knowledge and Risk-based. Additionally, the developed extension will also use OAuth 2.0 and Firebase Authentication. The study will be limited to testing the proctoring tool with online exams that are accessed using Google Forms. In addition, implementing and testing the proctoring tool will involve monitoring and collecting data on the student's digital identity and browsing activity during assessments. The collection of data will comply with Republic Act 10173 Data Privacy Act Of 2012 and include a data privacy consent form. Additionally, the proctoring tool will only be tested on Google Chrome because the proctoring tool may have compatibility limitations with other browsers.The proctoring tool's features are limited to what is stated in the methodology and is focused on monitoring student browser activity during online assessments. It cannot detect cheating methods that are outside the scope of the Chrome Extension API, such as using separate devices or external assistance.

REVIEW OF RELATED LITERATURE

There are several commercially available online proctoring applications. Furthermore, there have been numerous studies on the features of these applications and their feasibility in helping educational institutions with online examinations. Similarly, many articles explore the use of non-commercial applications with different authentication and proctoring methods. Most of these studies and applications on online proctoring tools focus on biometric authentication and the use of artificial intelligence to verify ID photos and track video recordings. Aside from that, online proctoring applications in these studies were developed with various authentication and authorization services such as Single sign-on, Firebase, and OAuth 2.0. Additionally, there are proctoring tools designed with learning management system (LMS) integration in mind, some of which are custom browsers and software that must be installed and run on specific hardware specifications. However, only limited studies and applications explore the use of browser extensions as proctoring tools for online examinations.

Authenticating Digital Identity

In a guidebook for OAuth2 and OpenID Connect written by Bertocci (n.d), Digital identity is defined as the set of attributes that describe a particular user within the context and scope of a particular application's function. For instance, in the case of a bookselling application, the user's credit card number, shipping address, and the most recent books they bought would all be the necessary set of attributes that will define the user. In their book, Riti (2018) also wrote that digital identity comprises e-mail addresses, bank details, and even third-party accounts such as Google and Apple. Given these definitions, the user's digital identity includes several characteristics that define and set them apart from other users. These characteristics will vary depending on the application's context and scope. According to Korac (2021), Users must have an online or digital identity to access the authentication process for using any e-learning platform. Additionally, digital identity in e-learning systems has gained considerable research focus. In the study of Korac et al. (2021), they defined digital identity as an individual's online presence and its associated information. They proposed a digital identity (MDI) model for managing and protecting personal information and improving information security management in e-learning systems.

Digital identity is knowing what attributes define the user. After knowing who the user is, the next step is the process of grabbing a set of credentials, sending it over to the application, and then checking if those credentials match the application's database. If they match, the user is authenticated (Bertocci, n.d). According to Flair (2023), authentication ensures that only those allowed to view or edit data on an application may do so. Moreover, authentication is the process of verifying the identity of an individual that is trying to access a service or resource. However, authentication should be distinct from authorization. According to Krebs (n.d), authorization is verifying what users can access or what actions they can perform. On the other hand, authentication is a process that requires proof of the user's digital attributes. In conclusion, Krebs (n.d) wrote that authentication leads to authorization but not the other way around. Academic institutions with online assessments should use an online proctoring tool to authenticate students' digital identities. By verifying the online identity of students, academic institutions can mitigate the risk of cheating during online exams.

Nguyen (2022) wrote a study on implementing Moodle Learning System to support the classroom in face-to-face and online remote learning. The study discussed the benefits of implementing Moodle, especially during the COVID-19 pandemic. In the study of Nguyen (2022), Moodle was described as an open-sourced learning management system that helps create online courses and content. Moodle allows easy access to course materials and assessments such as quizzes and exams. Overall, Moodle can help ensure an effective system for remote learning. One key feature of Moodle mentioned in the study (Nguyen, 2022) is its authentication system. Moodle has its own authentication system that can be used with several authentication plugins (Moodle Documentation, n.d.). Moodle can implement different authentication methods depending on the educational institution's needs. In the case of Nguyen's (2022) study for implementing Moodle for Keiwa College, they used Moodle's feature to augment itself with Google's secure login. Keiwa College already uses Google Education G-Suite as its digital workspace provider, so the integration enhances the security and privacy of the student's login credentials. To access Moodle resources, students must log in using their Google ID OAuth 2.0 credentials. This authentication method works when a user logs in to Moodle via Google, then Google's Authorization server will check if the entered credentials are valid, and once valid, an access token is issued, and the user will now be authenticated to use Moodle. Moodle uses this access token for any internal services that require a resource from the service provider (access to Moodle Course Content, e.g.) (Moodle Documentation, n.d.).

Another paper written by Okada et al. (2019) studied an online authentication system framework with functions to check identity and authorship in online examinations. The authentication system is called the Trust-based e-Assessment System for Learning (TesLA). It was provided for institutions to ensure legitimacy in e-assessment processes in online and blended environments. Okada et al.'s (2019) study focused on checking the efficacy of using TesLA and examining student attitudes towards authentication using the TesLA system. To check student authentication and authorship, TesLA combined different authentication methods. The TesLA system has knowledge, biometrics, possession, and mechanism-based security authentication for e-assessments. TesLA will ask for passwords, User IDs, and security questions for knowledge-based authentication based on the student's knowledge of confidential information. They also added biometrics and possession types of authentication based on the student's physiological and behavioral characteristics. Another authentication method is called mechanism, which tells where and when a student is, such as the examinee's location, a timestamp, or IP address.

Falana et al. (2020) presented a study that analyzes different authentication methods to enhance the security of learning management systems (LMS) for smart schools. The authentication system designed in their research combined three authentication methods: OAuth 2.0, 2-Factor Authentication (2FA), and Username and Password. In implementing their learning management system (LMS), users can access it if they sign up through an OAuth 2.0 protocol provider such as Facebook, Google, Twitter, and more. OAuth 2.0 will allow the learning management system to securely use the information from the social media accounts to log in or create accounts. Another method to access the learning management system (LMS) that Falana et al. (2020) used is through Username and Password. To create an account and log in to the LMS successfully, the user must have at least seven characters that mix one or more numeric, uppercase, and lowercase characters. For implementing the 2-Factor Authentication, Falana et al. (2020) gave users two options to authenticate: through a 6-digit code given through e-mail or Google Authenticator's time-based 6-digit to 8-digit One-Time password.

The works mentioned so far in this review of related literature focus on identifying a user's digital identity and providing users access using different authentication and authorization methods. However, knowledge-based information such as e-mail, student numbers, and answers to security questions can be stolen. Additionally, suppose the Google or Facebook account of the user is compromised. In that case, malicious users can use those credentials to log in to pretend to be the user. Another authentication method that protects users against these attacks is called Risk-based authentication (RBA). Risk-based authentication examines the credentials and other factors, such as the device, location, and network, when the user is logging in. The system will then decide whether to provide access, request a different credential, or deny access to the user entirely.

According to the study by Wiefling et al. (2022), Risk-based authentication will calculate a risk score to recognize suspicious login attempts. The risk score is based on monitoring unique features or information provided once the user tries to log in. Some of this information includes the IP address, geolocation, device, browser, and operating system, which are sent in the User-Agent HTTP header or call. The risk score will then inform the user of any other information they can give to gain access to the application. In Wiefling et al.'s (2022) study of evaluating and enhancing risk-based authentication, they gave different weights to certain features. Features that are harder to imitate are given more significant scores. The subfeatures of an IP address were given the following weights, IP address: 0.6, Autonomous System Number: 0.3, and country: 0.1. For the User-Agent feature, these were the given weights: Full string: 0.55, browser: 0.29, Operating System: 0.15, and device type: 0.01. In another previous study by Wiefling et al. (2020), they selected five features that scored highest in terms of how they can distinguish another user from another. The features were IP address, User-Agent string, language set, login time, and the device's display resolution. This study also found that IP addresses were a significant indicator for assessing the risk of login attempts. All the studies by Wiefling et al. (2020, 2022) highlighted the use of risk-based authentication in identifying suspicious login tries and the importance of considering multiple features, such as IP address and User-Agent string, in assessing login attempts.

Many authentication methods were mentioned in this review; however, building an application or tool with multiple authentication methods is complicated. Development can be simplified using Backend-as-a-Service models that allow the integration of multiple authentication methods and make database management more accessible. Numerous examples of studies and applications use Backend-as-a-Service models, specifically, Firebase.

One example is a mobile application Dhiman et al. (2019) developed called Breeze, which allows students to share ideas with fellow students. It is also a mobile application that allows real-time updates related to the events from the university. The Breeze mobile application is also a platform where students can view daily updates about their attendance, course syllabus, and timetable. This application also utilized some of the many services of Firebase, such as the NoSQL Real-time Database and Authentication. To access Breeze, users can be authenticated in Firebase through e-mail and password or using their Google or Facebook accounts. Likewise, Kapoor et al. (2020) proposed a mobile application that will allow students in middle school to learn using augmented reality. This mobile application is designed to provide an interactive learning experience for students. In addition to allowing students to view interactive newspapers, the application will allow students to use augmented reality to view a three-dimensional solar system model on their smartphone. Furthermore, the mobile application will use Firebase for its authentication module. The authentication process for this application involves the user providing their e-mail, password, and phone number for a Time Password (OTP). Additionally, the authentication process uses the Firebase API to store user login information and timestamps for each session where the students were actively using the mobile application. In addition, an application developed by Sharma et al. (2022) for their college utilized Firebase as a mobile Backend-as-a-Service (BaaS). The developed mobile application, MCCApp, uses many Firebase services such as authentication, NoSQL Real-time database, Cloud Storage, Crashlytics, A/B testing, and more. Additionally, Ntantinakis (2019) developed an application named CORE. This distance learning application would allow students to learn from their homes and places of employment and finish the course on their schedule. Their application used Firebase Authentication to authenticate the user to access the learning application courses and any other features. Firebase Authentication works by using the e-mail and password combination in this application. Lastly, Sukmana et al. (2020) proposed a gamified online quiz system that uses database technology to manage real-time data updates. They made use of two database technologies, Cloud Firestore, and CouchDB. The research evaluated their costs and how well each technology handled real-time data changes. The findings showed that Cloud Firestore outperforms CouchDB regarding latency and is more affordable.

In this review of related literature, different studies showed what different authentication methods were used to verify a student's digital identity. As mentioned, Okada et al. (2018) incorporated knowledge-based, biometric, possession-based, and mechanism-based authentication for online assessments, Falana et al. (2020) used OAuth 2.0, and Ntantinakis (2019) used Firebase Authentication. Additionally, studies by Wiefling et al. (2019, 2022) showed how Risk-based authentication can distinguish different users and secure each login attempt. These studies showed that combining different user profile attributes and then authenticating them using different combinations of authentication methods can enhance web authentication and reduce the risk of digital identity impersonation. Most applications were developed for educational institutions or to augment learning. The proposed proctoring tool in this study aims to authenticate students' digital identity using Multi-factor Authentication with Knowledge-based, OAuth 2.0, Risk-based, and Firebase. to strengthen authentication and reduce the risk of digital identity impersonation.

Proctoring Browser Activity

Online exam proctoring tools incorporate various technologies to monitor student behavior during remote exams. These tools often use screen recording, webcam monitoring, and artificial intelligence to detect suspicious activity. However, proctoring tools available on the market are costly. Additionally, current studies that focus on developing online assessment proctoring tools do not extensively explore using the Browser Extension API. A paper by Bergmans et al. (2021) studied the efficacy of Proctorio, one of the commercially-available online proctoring systems. Proctorio was chosen because it can be installed as a Google

Chrome extension, making it compatible with most operating systems. This browser extension offers different proctoring features, such as not allowing the opening of new browser tabs, recording of screen and audio, and restricting access to copy-paste. Proctorio has other features, such as identity verification, plagiarism detection, and web camera recording during an exam. According to the findings of Bergmans et al. (2021), Proctorio did not detect any cheating during the experiment. However, the human reviewers detected one of the six cheaters intentionally sampled for this study. This result means that Proctorio has a high percentage of false negatives. In addition, Students who were part of the sampling were also concerned with their privacy when it came to storing their video recordings. There is also a proctoring tool for online examinations called Honorlock. Honorlock is a program with a feature that flags suspicious behavior while administering an online examination. Purpura et al. (2021) proposed using Honorlock as a solution for a secure test administration of the online placement test for the Community English Language Program (CLP) at Teachers College, Columbia University. In the context of Purpura et al. (2021) 's study, they used Honorlock's live proctoring via web camera and microphone feature. During an online examination, Honorlock's artificial intelligence will flag suspicious behavior detected on the web camera and microphone, such as leaving the room, the presence of another person, or unnecessary audio. Each flagged behavior will be available for review in a post-administration proctoring report. This proctoring report will include information about the examinee and the incident when a suspicious event was flagged. The results of Purpura et al. (2021) 's study found that, in some cases, the sound file included in the report was corrupted. Another concern raised was privacy and the need for extra technical help.

In a study conducted by Kariyawasam et al. (2021), they proposed an online examination proctoring tool with automated cheating detection. The researchers used web camera monitoring with Convolutional Neural Networks to recognize and detect face spoofing. The proctoring system Kariyawasam et al. (2021) developed has a chromium-based extension and a desktop application. The desktop application has user verification and face spoofing detection features. On the other hand, the browser extension provides an added layer of proctoring by monitoring browsing activity. The browser extension can monitor students' activity while taking the online assessment, such as the currently active tab, resizing the window size, and opening a new tab. The real-time monitoring of the student's browsing behavior will detect possible attempts to access online resources while taking the test. The browser extension will then send a report back to the desktop application. Another browser extension developed by Makhlouf et al. (2022) called Track-ThinkTS captures different user behavior while using a web browser. They developed this extension to track students' web search behavior and thought process when they have to solve programming problems. The ThinkTS tracks actions like creating new browser tabs, closing browser tabs, copying from the clipboard, and when those actions were performed. It also tracks website information, such as the page's title, the page's URL, and the page's content where the action happened. During the testing of the ThinkTS extension, it was able to capture several types of user actions. ThinkTS utilized the Browser Extension API to capture user actions related to tabs management, clipboard usage, and website data while using a web browser.

Browser Extension API was used in both studies written by Makhlouf et al. (2022) and Kariyawasam et al. (2021) to collect the necessary user browser activity that they need for their respective studies. Commercially-available proctoring tools such as Proctorio and Honorlock were also used as browser extensions in Bergmans et al. (2021) and Purpura et al.'s (2021) studies. The Browser Extension API allowed their systems to communicate with the browser to collect real-time browsing data to monitor user browsing activity. All these studies showed that tracking a user's browsing behavior can be done using the Browser Extension API, and the tracked activity can be used for monitoring students while taking an online assessment. However, as mentioned in this review of related literature, some studies need to explore the use of the Browser Extension API extensively. The research written by Makhlouf et al. (2022), Kariyawasam et al. (2021), Bergmans et al. (2021), and Purpura et al. (2021) primarily focused on the tab management and clipboard tracking features of the Browser Extension API. The proctoring tool in this study will also use the Browser Extension API, specifically the Chrome Extensions API, to track other user activity and information, including the User-Agent string, CPU information, and display metadata. Overall, the studies and systems presented in this review would aid the development of the proctoring tool. The features and design of the proctoring tool will rely on the features mentioned in this review. The proctoring tool will have Multi-factor Authentication to strengthen authentication and use the Chrome Extension API to monitor student browsing activity while taking the online assessment.

METHODOLOGY

The proctoring tool was developed as a browser extension that is used alongside online exams conducted on Google Forms. Browser extensions are software programs that provide users to customize their browsing experience (Chrome Developers, 2022). The proctoring tool is installed on the Google Chrome browser.

Development Tools

The proctoring tool was developed on a machine with the following specifications:

- Operating System
  - Windows 11 64-bit
- Processor
  - AMD Ryzen 5 5600H with Radeon Graphics
- Memory
  - 16 GB DDR4
- Browser
  - Google Chrome 125.0.6422.142 64-bit

The proctoring tool was developed using the following software development tools and technologies:

- Visual Studio Code
  - A text code editor that was used as the Integrated Development Environment for developing the browser extension.
- Javascript

    - The scripting programming language of the web

- Firebase
    - A Backend-as-a-Service platform that provides a wide array of services for various applications built for the web or mobile. This tool used the following Firebase services
        - Authentication
        - Real-time Database
        - Firestore
        - Cloud Functions
        - Trigger Email Extension
- Google Cloud Platform
    - Allowed the proctoring tool to use Google OAuth 2.0 as its authentication provider
- Chrome Extension API
    - A platform that allow developers to extend the functionality of a browser. Chrome Extensions API is a programming interface that provides documentation for developing extensions for Chrome.

Types of Users

There are three types of users that will use this proctoring tool:

1. Student
    - The student has to be registered and authenticated to use the proctoring tool:

- The student’s digital identity is composed of the following information:
    - IP Address
    - Geolocation
    - Browser
    - Operating System
    - System Display Resolution
    - System CPU
- The student will receive an email about the details of their examination
- The student will be given the link to their online examination after they input the exam code and has been authenticated by the proctoring tool
- The student’s browser will be monitored such as:
    - websites visited in the current session
    - browser tabs that are newly opened
    - opening another tab
    - minimization of the browser
    - copy-paste action

2. Faculty-in-Charge (FIC)
    - The FIC has to be authenticated to use the proctoring tool
    - The FIC will be able to schedule online examinations and will be asked of the following:
    - The FIC will be given a 6-string assessment access code that is automatically emailed to their students

- The FIC can view the assessments they scheduled
- The FIC can view proctoring reports

3. Admin

- The admin has to be authenticated to use the proctoring tool:
- The admin can add faculty members and will be asked the following:
- The admin can add courses handled by faculty members
- The admin can upload the class list of a certain course. The class list is encoded as a csv file
- The admin can schedule online examinations for faculty members and will be asked of the following:
- The admin will be given a 6-string assessment access code that is automatically emailed to the students taking the exam
- The admin can view all the assessments scheduled in the proctoring tool
- The admin can view all the proctoring reports
- The admin can view all the faculty registered in the proctoring tool
- The admin can view all the students registered in the proctoring tool

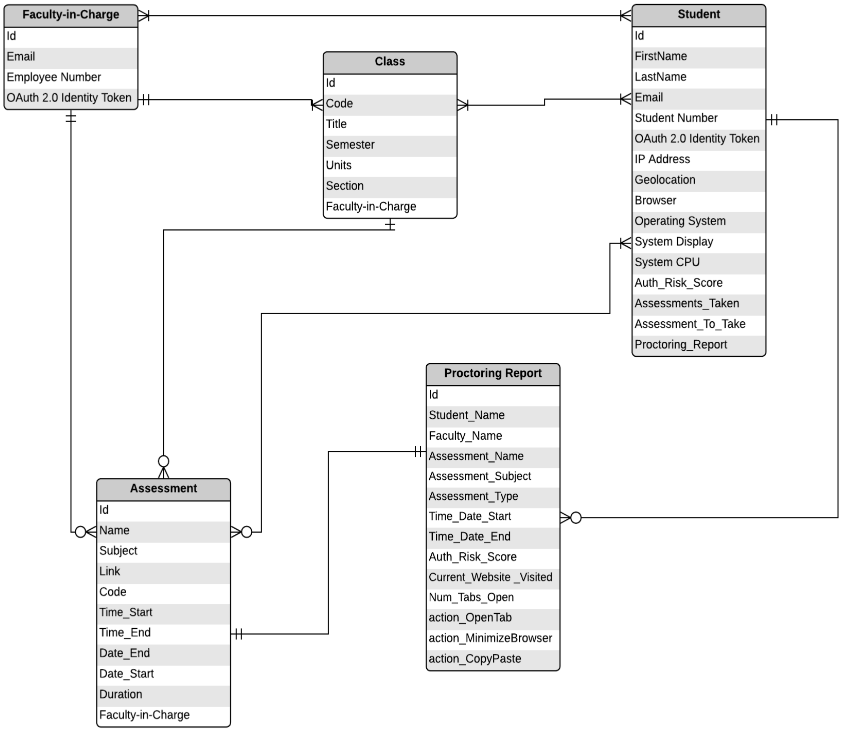


Figure 1. Entity Relationship Diagram (Crow's Foot Notation) of the Proctoring Tool

Features

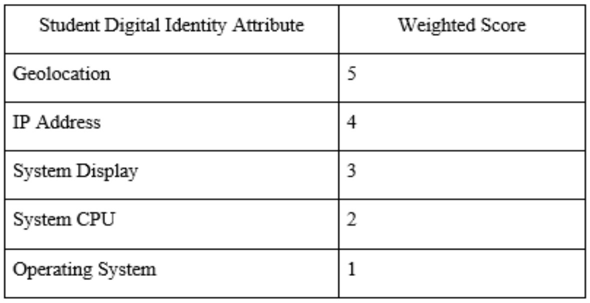
1. Multi-factor Authentication

   - In order to verify the student taking the assessment, the proctoring tool will gather data from the student. The information gathered are the following, but not limited to: institutional email account, student identification number, assessment code given by the Faculty-in-Charge, the student's IP address, Google Identity OAuth 2.0 token. The institutional email account and student identification number will ensure that the student taking the assessment is part of the institution, additionally, the results of the assessment will be linked to this student's account. The assessment code given by the Faculty-in-Charge is another layer of authenticating the student, this will make sure that the student is taking the right assessment scheduled by the Faculty-in-Charge.

- Another layer of authentication is using a Weighted Risk Scoring Model for Risk-based Authentication (Wiefling et al., 2020, 2022). By evaluating the different digital identity attributes involved with each login attempt of the student, Risk-based authentication can detect suspicious behavior such as identity spoofing. Each attribute of the student will be given a weight factor and will be compared to the data stored in the database. If the result from computing the Weighted Risk Score is less than 0.90, The student will still be allowed to take the exam but will be flagged as a suspicious attempt. On the other hand, if the Weighted Risk Score is greater than or equal to 0.90, the student will not be flagged as a suspicious user. The Weighted Risk Score is computed using this formula:

$$AuthRiskScore = \frac{Total\ Weight\ of\ Attributes\ Matched}{Total\ Weight\ of\ Attributes}$$

Figure 2. Formula for Authentication Risk Score



Student Digital Identity Attribute	Weighted Score
Geolocation	5
IP Address	4
System Display	3
System CPU	2
Operating System	1

Table 1: Weighted Risk Scoring for each Student Attribute

2. Proctoring

- Monitoring student activity in online assessments is challenging because proctoring is done remotely or not done at all because of the remote nature of online assessments. One of the objectives of this tool is to utilize the Browser Extension API in monitoring student activity while taking the assessment to flag possible cheating. To monitor student activity, the proctoring browser extension will track browser activity such as, but not limited to, the website visited in the current session, open browser tabs, attempts to open another tab, minimization of the browser, and the time the online assessment was accessed and submitted. The browser activity tracked by the extension will be stored in an activity log report only accessible to the Faculty-in-Charge. This report can be accessed in cloud storage and emailed to the Faculty-in-Charge.

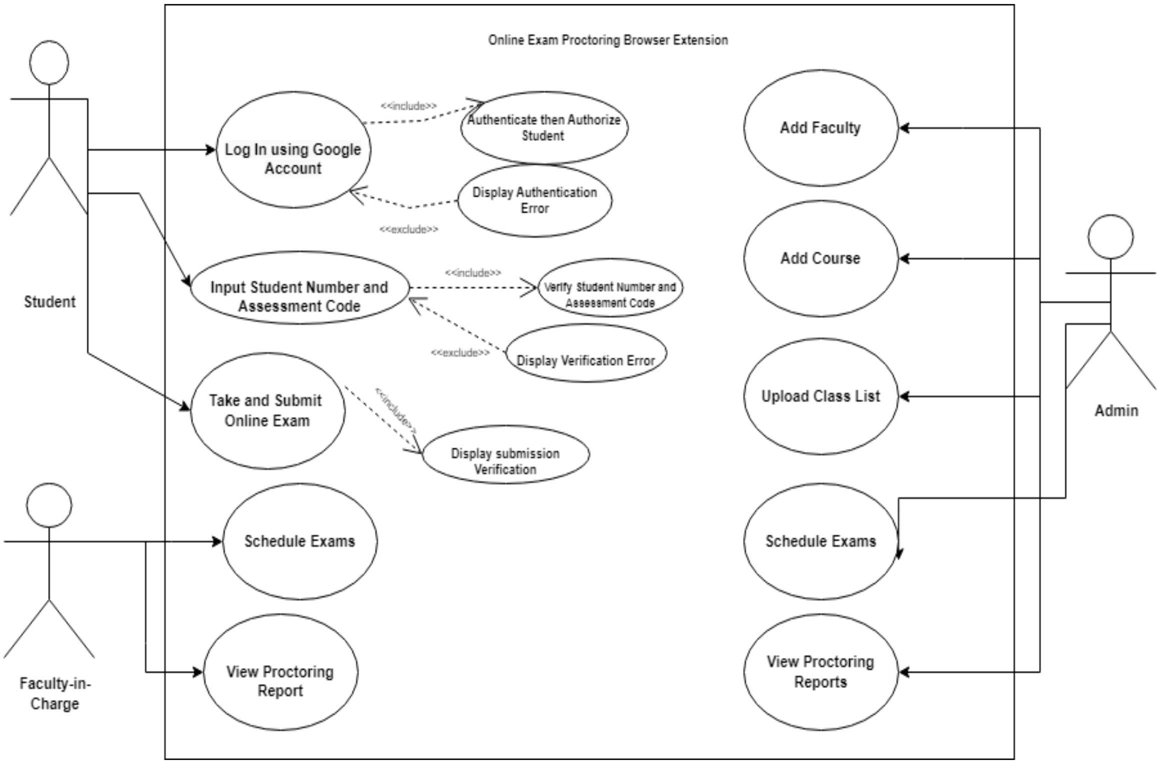

Online Exam Proctoring Browser Extension
Student
Log In using Google Account
<<include>>
Authenticate then Authorize Student
Display Authentication Error
<<exclude>>
Input Student Number and Assessment Code
<<include>>
Verify Student Number and Assessment Code
<<exclude>>
Display Verification Error
Take and Submit Online Exam
<<include>>
Display submission Verification
Faculty-in-Charge
Schedule Exams
View Proctoring Report
Add Faculty
Add Course
Upload Class List
Schedule Exams
View Proctoring Reports
Admin

Figure 3. Use Case Diagram of the Proctoring Tool

RESULTS AND DISCUSSION

Development Stage

The browser extension was developed using JavaScript, CSS, and HTML for the user interface. In addition, Chrome's sidePanel API was used to load the proctoring tool alongside the main content of the browser. This sidePanel API is a component of the Chrome Extensions API. It enables the proctoring tool to monitor browser activity and manipulate the Document Object Model (DOM) of the currently displayed webpage in the Chrome browser. Firebase Authentication and Google Identity were used to implement multi-factor authentication. Google Identity uses OAuth 2.0 tokens, which allow users to sign in using their institutional UP Gmail accounts. The Weighted Risk Scoring model was also implemented as an additional layer of authentication. The proctoring tool computed the scores by collecting a student's digital identity attributes upon registration and then comparing them to the digital identity attributes that the student had before taking the exam as shown in Figures 19 and 2o. Moreover, the browser extension used other Firebase services, such as its Realtime database, Cloud Firestore, and Trigger Email extension. Students scheduled to take the exam received automatic emails with exam details and codes through the Trigger Email extension.

However, certain limitations were met while developing the proctoring tool as a browser extension for all Chromium-based browsers. The multi-factor authentication process requires the OAuth 2.0 token from Google. The token grants access to various Google services, but due to security and privacy concerns, Chromium browsers have restricted its generation. As a result, the proctoring tool was developed exclusively for Chrome browsers. Nonetheless, Chrome extensions can be ported to a certain browser, given that other authentication methods are to be used. In addition to that, there were limitations encountered with Firebase. Initially, the free Spark plan was used, but the Trigger Email extension requires a Blaze plan. Despite this, the Blaze plan operates on a tier system, requiring payment only upon exceeding specific thresholds. The threshold for Firebase authentication is up to 50,000 monthly active users; for Cloud Firestore, it has a limit of 50,000 reads and 20,000 writes per day; for Realtime Database, it has a limit of 1 GB of storage and 10 GB for downloads; and for Trigger Email extension function invocations, the limit is 2 million per month. The security rules were updated for the Realtime database and Cloud Firestore to restrict access to data intended only for specific users.

The proctoring tool tracked various browser activities, such as websites visited during the current browser session, the number of newly opened tabs and their corresponding URLs, the number of switches from a Chrome window to another or window minimization, and the number of copy or paste actions detected. Additionally, the proctoring tool was able to generate reports about the browser activity and the authentication review for each student who took an exam. Lastly, the proctoring tool also generated a summary proctoring report for each exam, containing detailed information about the total number of examinees, submissions, students with and without flagged activity, and students with the most matching and non-matching authentication factors based on their digital identity.

Administrator-side of the browser extension

Administrators are required to log in using their UP Gmail accounts. Additionally, administrators have to input a unique identification number. The administrator is capable of using the following functions:

1. Manage Faculty - Administrators can add a new faculty member to the database.
2. Add Course to Faculty - Administrators can add courses that a particular faculty teaches.
3. View All Courses - Administrators can view all the courses listed in the database.

4. Upload Class List - Administrators can upload the class list in CSV format for each class taught by the faculty.
5. Manage Students - Administrators can view all the students added to the database.
6. Manage Exams - Administrators can schedule and view all the exams in the proctoring tool.
7. Schedule Exams - Administrators can schedule exams for a particular faculty member for their respective class.
8. View Proctoring Report Summary - Administrators can view the summary of the proctoring report for an exam, which displays detailed information about the total number of examinees, submissions, students with and without flagged activity, and students with the most matching and non-matching authentication factors based on their digital identity.
9. View Student Proctoring Report Details - Administrators can view a report that displays the time started, time submitted, number of flagged browser activities, which browser activities were detected during the browser session, and whether new tabs were opened.
10. View Student Authentication Report - Administrators can view the individual authentication report for each student. The report will display the Auth Risk Score and Authentication Status, which are the results of computing the Weighted Risk score, and the Digital Identity Match Status, which shows which attributes of the student's identity were matched from registration and upon taking the assessment and which attributes changed.

Faculty-side of the browser extension

Faculty members must log in with their UP Gmail accounts. Next, they have to enter their unique employee number. Faculty users are capable of using the following functions:

1. Schedule Exams - Faculty users can schedule exams for their classes.

2. Send Email Notification - Faculty users can automatically send an email to their students containing the unique exam access code and other exam details.

3. View Exams - Faculty members can access and view all the exams they have scheduled.

4. View Proctoring Report Summary - Faculty users can access and view a summary of the proctoring report for an exam. The report is similar to the administrator-side.

5. View Student Proctoring Report Details - Faculty users can view a report that displays the time the student started the exam, the time it was submitted, the number of flagged browser activities, the specific browser activities that were detected during the exam session, and whether any new tabs were opened.

6. View Student Authentication Report - Faculty users can access and review the individual authentication report for each student. The report will display the Auth Risk Score and Authentication Status, which are the results of calculating the Weighted Risk score, and the Digital Identity Match Status, which indicates which attributes of the student's identity were matched from registration and upon taking the assessment, as well as any changes in those attributes.

Student-side of the browser extension

Students must first authenticate and register in order to access their online exams.

1. Authentication Process

    - Login with an Institutional Google Account - Students are required to log in with their UP Gmail accounts.

    - Enter Student Number - After logging in, students must enter their student number.

- Once a faculty member schedules a student's exam, they will receive an email containing the following exam details:
    - Exam Access Code - A unique code to access an exam.
    - Exam Schedule - The exam's start and end times and dates.
    - Exam Details - Name, Course and Section, Faculty-in-Charge

2. Taking an exam
    - Students can input the exam access code they received in their email. If a student attempts to access an exam that is not scheduled for them or that is outside the scheduled time, they will not be able to access the exam.
3. Accessing the Online Exam Link
    - Once the student has verified the exam details, they can click on the provided link to access their exam.
    - Open Exam - The exam link will open in their current browser window, and they can begin taking the exam.
    - Time Duration - The proctoring tool will display the details about the exam currently being taken as well as a countdown timer.
4. Submission of the Exam
    - Submit in the Learning Management System - Students can submit their completed exam within their Learning Management System (LMS).
    - Submit in the Proctoring Tool - To finalize their submission, students would have to go back to the proctoring tool and click the ”Submit Exam” button to finalize their submission. This will also close the online exam.
5. Completion of an Exam

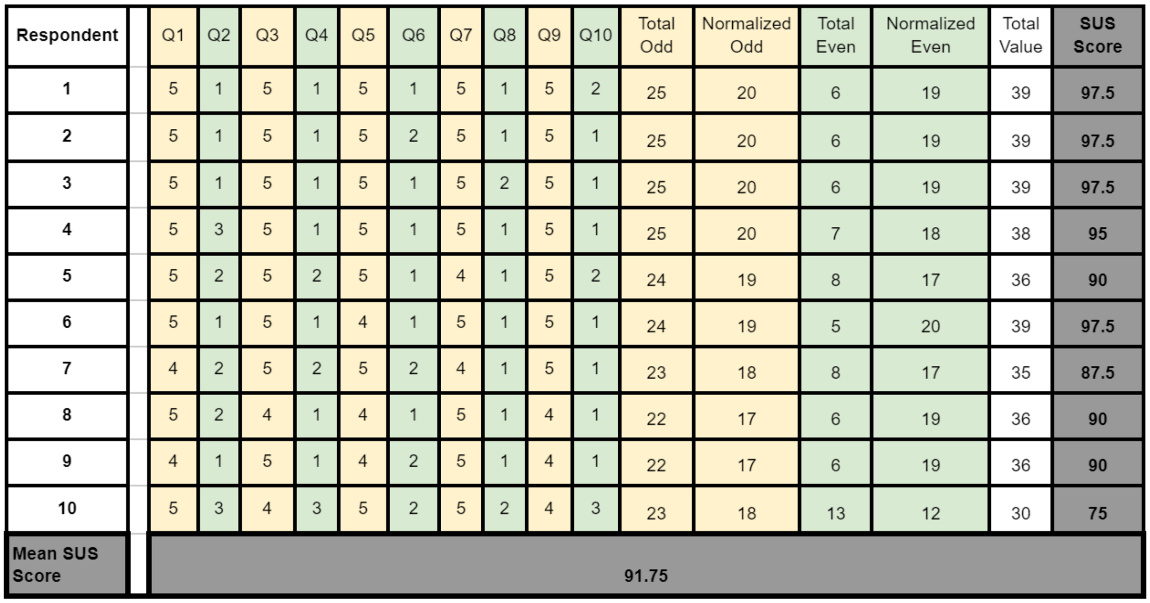
- Students can view the number of browser activities recorded during their exam session.

System Usability Testing

The proctoring tool, AuthoExam was tested by 10 respondents, who are constituents of the UP system. The respondents have experienced taking or scheduling an online exam. The System Usability Scale (SUS) was used to measure the usability of the proctoring tool. The System Usability Scale consisted of 10 statements with a five-point scale that ranged from ”Strongly Disagree” to ”Strongly Agree.” The statements were the following:

1. I think that I would like to use this system frequently.
2. I found the system unnecessarily complex
3. I thought the system was easy to use.
4. I think that I would need the support of a technical person to be able to use this system.
5. I found the various functions in this system were well integrated.
6. I thought there was too much inconsistency in this system.
7. I would imagine that most people would learn to use this system very quickly.
8. I found the system very awkward to use.
9. I felt very confident using the system.
10. I needed to learn a lot of things before I could get going with this system.

The individual scores were calculated once the respondents completed the survey. The scores are calculated by subtracting 5 from the points for all odd-numbered questions and then adding it to 25 minus the sum of the points for all even-numbered questions. The output of the calculation will be multiplied by 2.5 in order to convert the initial scores to a range of 0-100. The individual scores and computation are shown in Table 2.



Respondent	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Total Odd	Normalized Odd	Total Even	Normalized Even	Total Value	**SUS Score**
1	5	1	5	1	5	1	5	1	5	2	25	20	6	19	39	**97.5**
2	5	1	5	1	5	2	5	1	5	1	25	20	6	19	39	**97.5**
3	5	1	5	1	5	1	5	2	5	1	25	20	6	19	39	**97.5**
4	5	3	5	1	5	1	5	1	5	1	25	20	7	18	38	**95**
5	5	2	5	2	5	1	4	1	5	2	24	19	8	17	36	**90**
6	5	1	5	1	4	1	5	1	5	1	24	19	5	20	39	**97.5**
7	4	2	5	2	5	2	4	1	5	1	23	18	8	17	35	**87.5**
8	5	2	4	1	4	1	5	1	4	1	22	17	6	19	36	**90**
9	4	1	5	1	4	2	5	1	4	1	22	17	6	19	36	**90**
10	5	3	4	3	5	2	5	2	4	3	23	18	13	12	30	**75**
Mean SUS Score	**91.75**															

Table 2. Results of the System Usability Scale Questionnaire

According to Sauro (2011), a score above 68 would be considered above average and anything below 68 would be below average. In addition to that, According to Bangor et. al. (2009) SUS scores can have an Adjective Rating Scale as shown in Figure 4. Given the following scales, the mean SUS score (91.75) computed for this proctoring tool is classified Above Average, Excellent and Acceptable.

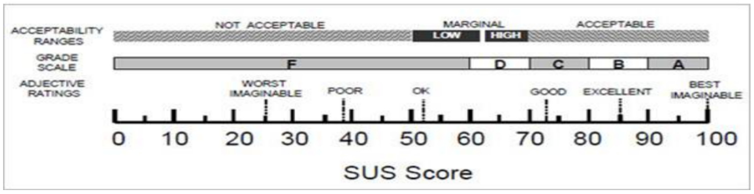


Figure 4. Adjective Rating Scale

CONCLUSION AND FUTURE WORK

AuthoExam is a browser extension that is developed to be a proctoring tool intended to help maintain and ensure the integrity of online examinations. The proctoring tool was created to authenticate the digital identity of students through the use of multi-factor authentication (MFA), utilizing knowledge-based factors like identification numbers and exam access codes.In addition, OAuth 2.0 tokens and risk-based authentication were implemented to verify the identity of the student taking the online assessment. The Chrome Extension API was used to real-time monitor student browser activity, which allowed the proctoring tool to flag potential cheating behaviors such as switching tabs, minimizing the browser window, and copying and pasting.

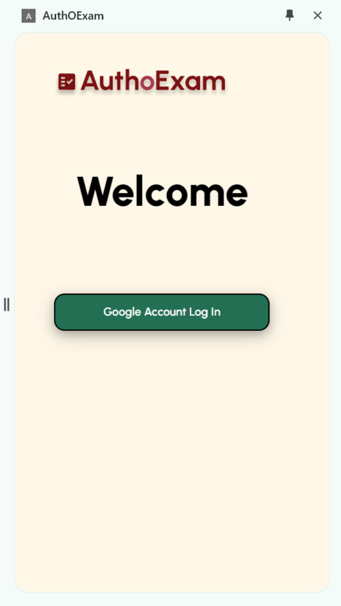
Three roles can access the proctoring tool: admin, student, and faculty, each with their own set of functionalities. The admin user can perform a wide range of tasks, such as adding faculty, adding courses, uploading class lists, scheduling exams, and viewing proctoring reports. Faculty members can use the proctoring tool to schedule exams for their classes and view proctoring reports. Finally, after faculty users schedule the exam, students can receive automatic emails, take the online exam using the provided link, and generate a proctoring report that their faculty-in-charge can view and access.

AuthoExam was evaluated using the System Usability Scale. There were 10 respondents who are constituents of the UP system. The respondents have experience taking or scheduling an online exam. The average SUS score computed for this proctoring tool was 91.75, which is classified as Above Average, Excellent, and Acceptable according to the descriptive scale (Bergmans et al., 2021). The mean SUS score of 91.75 also infers that the proctoring tool was found highly usable by the respondents, who are users who have experienced taking or scheduling online exams.

For future work, it is recommended to port the proctoring tool as a browser extension that can be installed on other browsers as well. In implementing a cross-browser extension,, a different method of multi-factor authentication and authorization should be implemented. Further improvements were also collected from the respondents. Respondents also recommended the addition of an ”Auto Submit” feature, which would automatically submit and generate a proctoring report in the proctoring tool right after an exam has already been submitted in the LMS or Google Forms. Future developers and researchers can also add other multi-factor authentication factors, such as One-time passwords or Inherence-based factors like keystroke dynamics.

APPENDIX I

Screenshots for User Interface

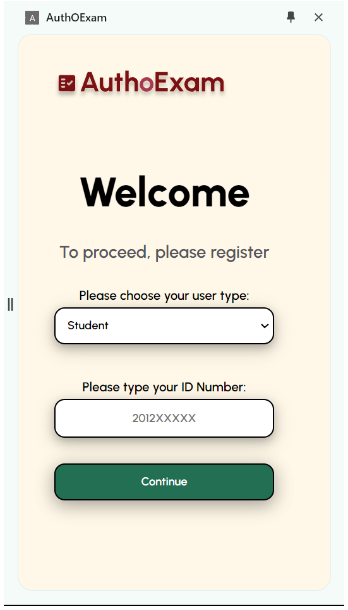


AuthOExam

AuthoExam

Welcome

Figure 5. Landing Page of AuthoExam



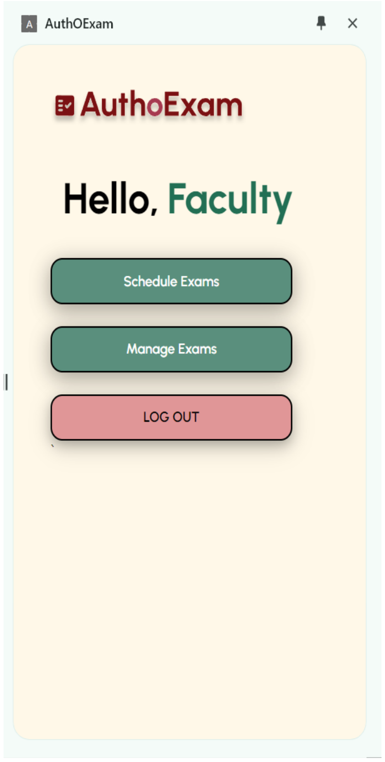
Welcome

To proceed, please register

Please choose your user type: Student

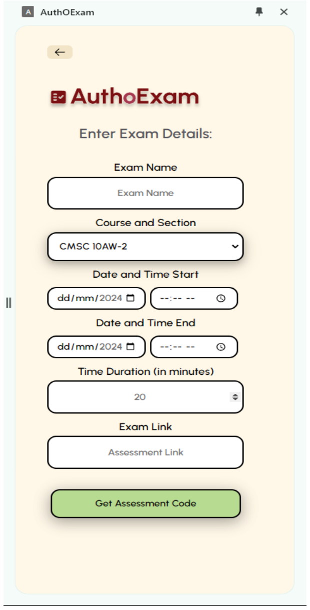
Please type your ID Number: 2012XXXXX

Figure 6. Input for Identification Number Page



Hello, Faculty

Figure 7. Faculty Dashboard Page


AuthOExam

AuthoExam

Enter Exam Details:

Exam Name: Exam Name

Course and Section: CMSC 10AW-2

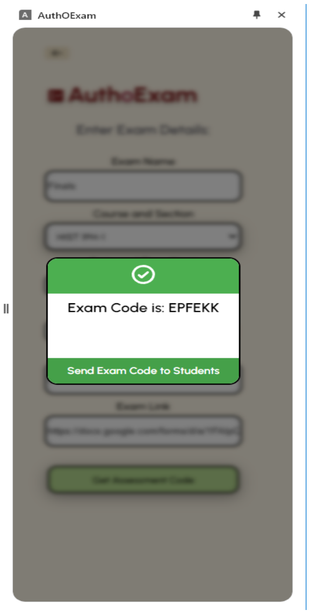
Date and Time Start: dd/mm/2024 --:-- --

Date and Time End: dd/mm/2024 --:-- --

Time Duration (in minutes): 20

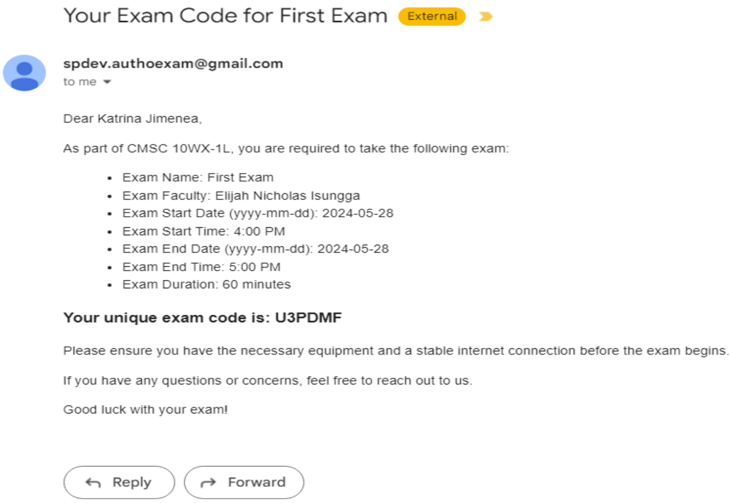
Exam Link: Assessment Link

Figure 8. Faculty Schedule Assessment Page


AuthOExam

Exam Code is: EPFEKK

Figure 9. Faculty is given the exam code



Your Exam Code for First Exam External

spdev.authoexam@gmail.com
to me

Dear Katrina Jimenea,

As part of CMSC 10WX-1L, you are required to take the following exam:

- Exam Name: First Exam
- Exam Faculty: Elijah Nicholas Isungga
- Exam Start Date (yyyy-mm-dd): 2024-05-28
- Exam Start Time: 4:00 PM
- Exam End Date (yyyy-mm-dd): 2024-05-28
- Exam End Time: 5:00 PM
- Exam Duration: 60 minutes

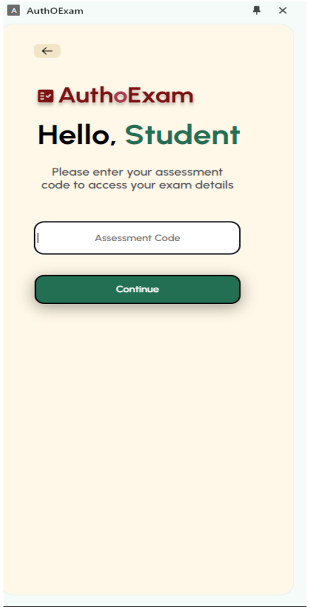
Your unique exam code is: U3PDMF

Please ensure you have the necessary equipment and a stable internet connection before the exam begins.

If you have any questions or concerns, feel free to reach out to us.

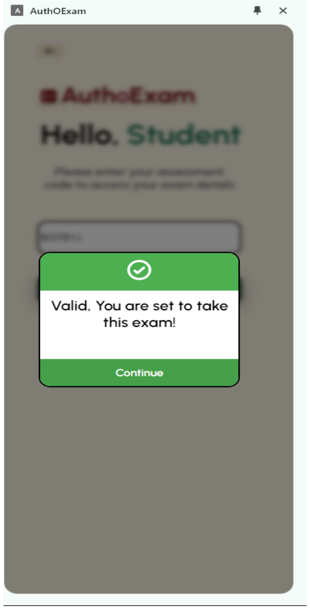
Good luck with your exam!

Figure 10. Student receives email



Please enter your assessment code to access your exam details

Figure 11. Student enters given exam code



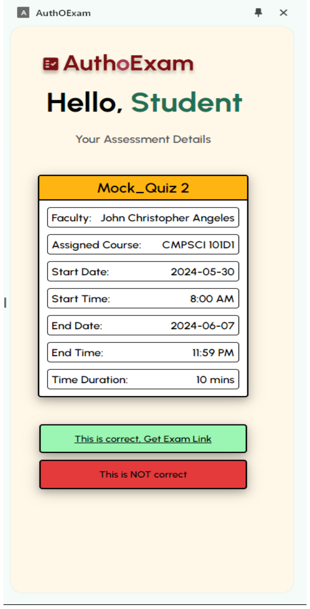
AuthoExam

Hello, Student

Please enter your assessment code to access your exam details.

Valid, You are set to take this exam!

Figure 12. Student is valid to take exam



AuthoExam

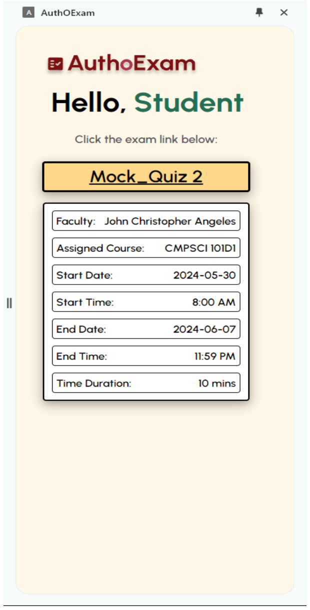
Hello, Student

Your Assessment Details

Mock_Quiz 2

Faculty:	John Christopher Angeles
Assigned Course:	CMPSCI 101D1
Start Date:	2024-05-30
Start Time:	8:00 AM
End Date:	2024-06-07
End Time:	11:59 PM
Time Duration:	10 mins

Figure 13. Student verify exam



AuthOExam

AuthoExam

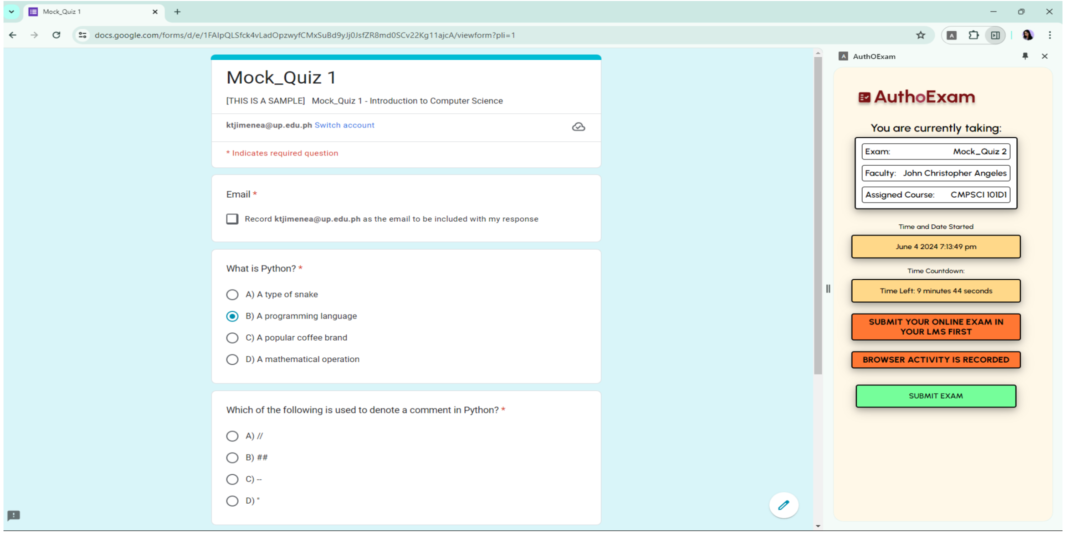
Hello, Student

Click the exam link below:

Mock_Quiz 2

Faculty:	John Christopher Angeles
Assigned Course:	CMPSCI 101D1
Start Date:	2024-05-30
Start Time:	8:00 AM
End Date:	2024-06-07
End Time:	11:59 PM
Time Duration:	10 mins

Figure 14. Student gets exam link



Mock_Quiz 1

docs.google.com/forms/d/e/1FAIpQLSfck4vLadOpzwyfCMxSuBd9yJj0JsfZR8md0SCv22Kg11ajcA/viewform?pli=1

Mock_Quiz 1

[THIS IS A SAMPLE] Mock_Quiz 1 - Introduction to Computer Science

ktjimenea@up.edu.ph Switch account

* Indicates required question

Email *

☐ Record **ktjimenea@up.edu.ph** as the email to be included with my response

What is Python? *

○ A) A type of snake

● B) A programming language

○ C) A popular coffee brand

○ D) A mathematical operation

Which of the following is used to denote a comment in Python? *

○ A) //

○ B) ##

○ C) --

○ D) "

AuthOExam

AuthoExam

You are currently taking:

Exam:	Mock_Quiz 2
Faculty:	John Christopher Angeles
Assigned Course:	CMPSCI 101D1

Time and Date Started

June 4 2024 7:13:49 pm

Time Countdown:

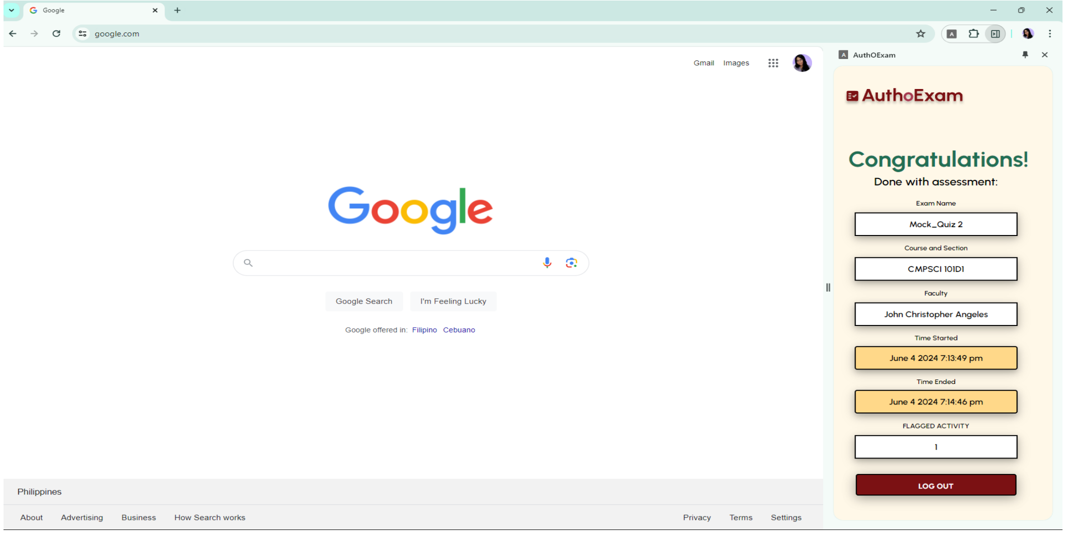
Time Left: 9 minutes 44 seconds

SUBMIT YOUR ONLINE EXAM IN YOUR LMS FIRST

BROWSER ACTIVITY IS RECORDED

SUBMIT EXAM

Figure 15. Student takes exam



AuthoExam

Congratulations!

Done with assessment:

Exam Name

Mock_Quiz 2

Course and Section

CMPSCI 101D1

Faculty

John Christopher Angeles

Time Started

June 4 2024 7:13:49 pm

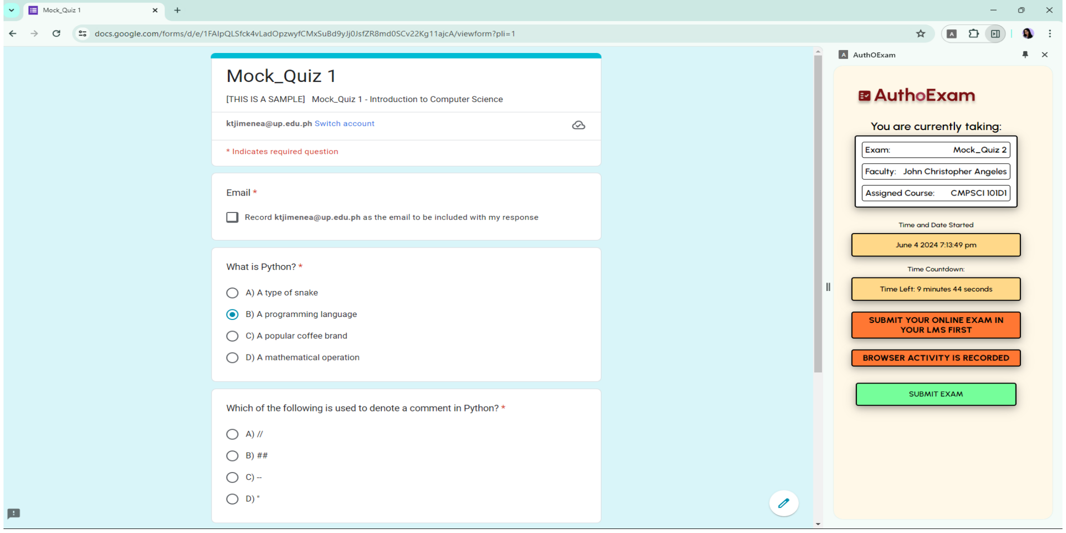
Time Ended

June 4 2024 7:14:46 pm

FLAGGED ACTIVITY

1

Figure 16. Student submits exam



docs.google.com/forms/d/e/1FAIpQLSfck4vLadOpzwyfCMxSuBd9yJj0JsfZR8md0SCv22Kg11ajcA/viewform?pli=1

Mock_Quiz 1

[THIS IS A SAMPLE] Mock_Quiz 1 - Introduction to Computer Science

ktjimenea@up.edu.ph Switch account

* Indicates required question

Email *

□ Record ktjimenea@up.edu.ph as the email to be included with my response

What is Python? *

○ A) A type of snake
● B) A programming language
○ C) A popular coffee brand
○ D) A mathematical operation

Which of the following is used to denote a comment in Python? *

○ A) //
○ B) ##
○ C) --
○ D) "

AuthoExam

You are currently taking:

Exam: Mock_Quiz 2
Faculty: John Christopher Angeles
Assigned Course: CMPSCI 101D1

Time and Date Started

June 4 2024 7:13:49 pm

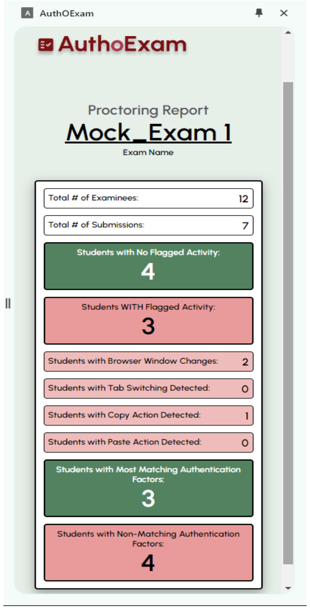
Time Countdown:

Time Left: 9 minutes 44 seconds

SUBMIT YOUR ONLINE EXAM IN YOUR LMS FIRST

BROWSER ACTIVITY IS RECORDED

Figure 17. Proctoring Report Summary



AuthOExam

AuthoExam

Proctoring Report

Mock_Exam 1

Exam Name

Total # of Examinees: 12

Total # of Submissions: 7

Students with No Flagged Activity: 4

Students WITH Flagged Activity: 3

Students with Browser Window Changes: 2

Students with Tab Switching Detected: 0

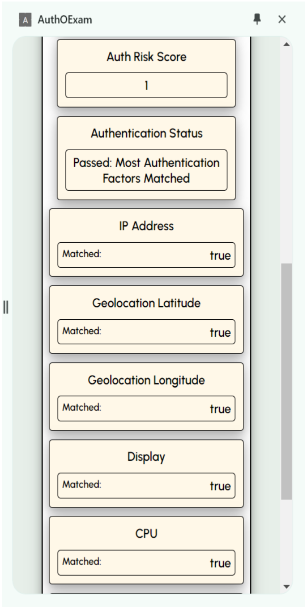
Students with Copy Action Detected: 1

Students with Paste Action Detected: 0

Students with Most Matching Authentication Factors: 3

Students with Non-Matching Authentication Factors: 4

Figure 18. Proctoring Report Summary



AuthOExam

Auth Risk Score: 1

Authentication Status: Passed: Most Authentication Factors Matched

IP Address — Matched: true

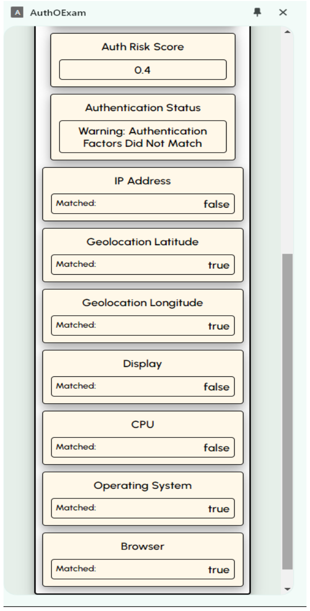
Geolocation Latitude — Matched: true

Geolocation Longitude — Matched: true

Display — Matched: true

CPU — Matched: true

Figure 19. Student Authentication Report where all digital identity attributes matched



Auth Risk Score
0.4

Authentication Status
Warning: Authentication Factors Did Not Match

IP Address
Matched: false

Geolocation Latitude
Matched: true

Geolocation Longitude
Matched: true

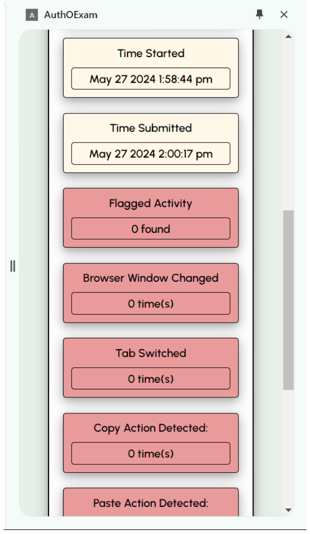
Display
Matched: false

CPU
Matched: false

Operating System
Matched: true

Browser
Matched: true

Figure 20: Student Authentication Report where most digital identity attributes did not match



Time Started
May 27 2024 1:58:44 pm

Time Submitted
May 27 2024 2:00:17 pm

Flagged Activity
0 found

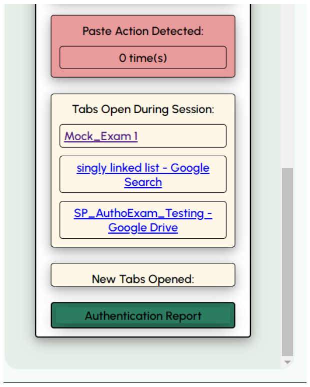
Browser Window Changed
0 time(s)

Tab Switched
0 time(s)

Copy Action Detected:
0 time(s)

Paste Action Detected:

Figure 21. Student Proctoring Report



Paste Action Detected:

0 time(s)

Tabs Open During Session:

Mock_Exam 1

singly linked list - Google Search

SP_AuthoExam_Testing - Google Drive

New Tabs Opened:

Figure 22. Student Proctoring Report with websites opened during the session

LITERATURE CITED

BANGOR, A., KORTUM, P., & MILLER, J. (2009). Determining what individual sus scores mean: Adding an adjective rating scale. *Journal of Usability Studies*, 114–123.

BERGMANS, L., BOUALI, N., LUTTIKHUIS, M., & RENSINK, A. (2021). On the efficacy of online proctoring using proctorio. *Proceedings of the 13th International Conference on Computer Supported Education*, *1*, 279-290. doi: 10.5220/0010399602790290

BERTOCCI, V. (n.d.). *Auth0 — oauth2 and openid connect: The professional guide.* Okta. Retrieved 2023-06-11, from https://auth0.com/resources/ebooks/oauth-openid-connect-professional-guide

DEVELOPERS, C. (2022, 10). *Chrome extensions 101.* Retrieved from https://developer.chrome.com/docs/extensions/mv3/getstarted/extensions-101/

DHIMAN, R., BASRAL, A., & JASWANTI. (0). *A new android application (breeze) for college management system.* doi: 10.1109/ICCMC.2019.8819787

DOCUMENTATION, M. (n.d.). *Authentication - moodledocs.* Moodle. Retrieved from https://docs.moodle.org/402/en/Authentication

FALANA, O. J., EBO, I. O., & ODOM, I. S. (2021). *Se-lms: Secured learning management systems for smart school.*

FIREBASE. (2019, 03). *Firebase authentication — firebase.* Retrieved from https://firebase.google.com/docs/auth/

FLAIR, I. (2023). *Electronic authentication.* Salem Press.

HODGES, C., MOORE, S., LOCKEE, B., TRUST, T., & BOND, A. (2020, 03). *The difference between emergency remote teaching and online learning.* Retrieved from https://er.educause.edu/articles/2020/3/the-difference-between-emergency-remote-teaching-and-online-learning

HUSSEIN, M. J., YUSUF, J., DEB, A. S., FONG, L., & NAIDU, S. (2020, 12). An evaluation of online proctoring tools. *Open Praxis*, *12*, 509. doi: 10.5944/openpraxis.12.4.1113

KAPOOR, V., & NAIK, P. (2020). Augmented reality-enabled education for middle schools. *SN Comput. Sci.*, *1*(3). Retrieved from https://doi.org/10.1007/s42979-020-00155-6 doi: 10.1007/s42979-020-00155-6

Kariyawasam, S., Lakshan, A., Liyanage, A., Gimhana, K., Piyawardana, V., & Mallawarachchi, Y. (0). *Standalone application and chromium browser extensionbased system for online examination cheating detection.* doi: 10.1109/ICAC54203.2021.9671103

Korać, D., Damjanović, B., & Simić, D. (2022). A model of digital identity for better information security in elearning systems. *The Journal of Supercomputing*, *78*, 3325-3354. Retrieved from https://doi.org/10.1007/s11227021039814 doi: 10.1007/s11227021039814

Krebs, B. (2019, 11). *The openid connect handbook.* Okta. Retrieved from https://auth0.com/blog/the-openid-connect-handbook/

Makhlouf, J., Arakawa, Y., & Watanabe, K. (2022). *A privacyaware browser extension to track user search behavior for programming course supplement.* Springer International Publishing.

Mphahlele, R. S. (2020). Online learning support in a ubiquitous learning environment. *Managing and Designing Online Courses in Ubiquitous Learning Environments*, 1-18. doi: 10.4018/978-1-5225-9779-7.ch001

Nguyen, P. (2022). A study on implementing moodle learning management system (lms) into the classroom. = *Bulletin of Keiwa College/ , (31), 95-108.*.

Ntantinakis, N. (2020, 05). Implementation of a serious educational web-based game for java programming tutorial. *apothesis.lib.hmu.gr*. Retrieved 2023-06-11, from https://apothesis.lib.hmu.gr/handle/20.500.12688/9410

Nurunnabi, M., & Hossain, M. A. (2019, 01). Data falsification and question on academic integrity. *Accountability in Research*, *26*, 108-122. doi: 10.1080/08989621.2018.1564664

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. Retrieved from https://bera-journals.onlinelibrary.wiley.com/doi/abs/10.1111/bjet.12608 doi: https://doi.org/10.1111/bjet.12608

Purpura, J. E., Davoodifard, M., & Voss, E. (2021). Conversion to remote proctoring of the community english language program online placement exam at teachers college, columbia university. *Language Assessment Quarterly*, *18*, 42-50. Retrieved from https://doi.org/10.1080/15434303.2020.1867145 doi: 10.1080/15434303.2020.1867145

Reedy, A., Pfitzner, D., Rook, L., & Ellis, L. (2021, 03). Responding to the covid-19 emergency: student and academic staff perceptions of academic integrity in the transition to online exams at three australian universities. *International Journal for Educational Integrity*, *17*. doi: 10.1007/s40979-021-00075-9

Riti, P. (2018). Identity and access management with google cloud platform. In (p. 223–244). Apress. Retrieved from `https://doi.org/10.1007/978-1-4842-3897-4` doi: 10.1007/978-1-4842-3897-4

'Sauro, J. (2011). *Measuringu: Measuring usability with the system usability scale (sus).* Retrieved from `https://measuringu.com/sus/`

Sharma, D., & Dand, H. (2019, 06). Firebase as baas for college android application. *International Journal of Computer Applications*, *178*, 1-6. doi: 10.5120/ijca2019918977

Solano, J., Camacho, L., Correa, A., Deiro, C., Vargas, J., & Ochoa, M. (2021). Combining behavioral biometrics and session context analytics to enhance risk-based static authentication in web applications. *Int. J. Inf. Secur.*, *20*(2), 181–197. Retrieved from `https://doi.org/10.1007/s10207-020-00510-x` doi: 10.1007/s10207-020-00510-x

Sujanani, T., & Vinod, S. (2018, 03). Implementation of openidconnect and oauth 2.0 to create sso for educational institutes. *International Journal of Engineering Technology*, *7*, 153. doi: 10.14419/ijet.v7i2.6.10142

Tentea, E.-C., & Ionescu, V. M. (2019, 06). *Online quiz implementation using blockchain technology for result tampering prevention.* Retrieved from `https://ieeexplore.ieee.org/abstract/document/9041980` doi: 10.1109/ECAI46879.2019.9041980

What is a session cookie? (n.d.). Retrieved from `https://www.cookiepro.com/knowledge/what-is-a-session-cookie/`

Wiefling, S., Iacono, L., & Dürmuth, M. (2019). *Is this really you? an empirical study on riskbased authentication applied in the wild.* Springer International Publishing.

Wiefling, S., Jørgensen, P. R., Thunem, S., & Iacono, L. L. (2022). Pump up password security! evaluating and enhancing risk-based authentication on a real-world large-scale online service. *ACM Trans. Priv. Secur.*, *26*(1). Retrieved from `https://doi.org/10.1145/3546069` doi: 10.1145/3546069