Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Real Time Online Exam Monitor Management System in Educational Institutions

Mona Esmat [1,*], Amira Atta[2], W. K. El Said[3]
[1] Lecturer, Computer Department, Mansoura University, Egypt
[2] Lecturer, Computer Department, Mansoura University, Egypt
[3] Associate Professor, Computer Department, Mansoura University, Egypt

Emails: monaesmat1980@gmail.com
Dr.amiraatta@mans.edu.eg
prof_wessam@mans.edu.eg

ARTICLE INFO **ABSTRACT**

Received: 14 Feb 2025
Revised: 25 April 2025
Accepted: 2 May 2025

Maintaining academic integrity in online examinations is a critical challenge within digital learning environments. This research presents an integrated, multimodal authentication system designed to detect and prevent cheating in real-time during remote assessments. The system combines secure identity verification, continuous facial recognition, audio analysis, and object detection to monitor student behavior comprehensively throughout the exam session. Before exam access, students undergo a rigorous identity verification process using pre-registered biometric data. During the exam, facial recognition continuously confirms the presence of the authenticated student. At the same time, audio classification identifies suspicious sounds such as whispering, paper rustling, or electronic device usage that may indicate unauthorized assistance. Simultaneously, object detection scans the video feed for prohibited items such as mobile phones or notes. All detected irregularities are immediately recorded in a real-time database, complete with timestamps and screenshots to serve as documented evidence. Repeated or prolonged violations trigger automatic flags for potential misconduct, facilitating review by academic integrity committees. The study sample consisted of 30 first-year Computer Department students from the Faculty of Specific Education at Mansoura University. Statistical analysis revealed a highly significant difference ($p < 0.01$) in students' achievement scores before and after the system's implementation, with higher scores observed before using the monitoring system. The large effect size (0.677) underscores the system's effectiveness in curbing cheating behaviors. Additionally, a reduction in score variability post-implementation suggests increased homogeneity and a general decline in performance, likely reflecting the system's stringent monitoring and its impact on limiting dishonest practices. By automating the detection of academic dishonesty and reducing reliance on human proctors, this system offers a scalable and reliable solution for enhancing the fairness and credibility of online examinations.

Keywords: Real-Time Online Exam; E-Exams; Abnormal Activities; Exam Management System; Exam Monitor.

1. INTRODUCTION

Exams can generally be separated into two categories: traditional and online. Online exams, conducted via the internet or an intranet, allow students or candidates to complete assessments using computers or internet-enabled devices, such as smartphones or tablets. Over time, online exams are anticipated to offer greater efficiency and cost savings compared to traditional paper-based exams. They provide the flexibility to accommodate large numbers of participants, and when automated grading systems are in place, results can be generated and accessed almost instantly, enhancing the overall testing experience [1],[2],[3]. The use of information technology can give rise to challenges and errors[4].Exams are a vital part of any educational program, with academic dishonesty typically handled administratively at either the classroom or institutional level; however, in online courses, cheating has become more accessible, with many students admitting to taking advantage of this ease through methods such as using online tools like Google to find answers, collaborating with peers during assessments, and consulting personal notes or course textbooks[5].

Impersonation in the context of examinations refers to a situation where one individual takes an exam on behalf of another, falsely presenting themselves as the legitimate candidate[6].Student identity verification is a term that refers to the process of verifying a learner's identity at various moments of their education. The goal is to ensure that the person who registers for a class, course, certificate, or degree — and who will receive the credential or credit associated with it — is the same person who completes the material. There are three categories of identity[7],[8]:

- Attributed identity involves your parents' names and your place of birth.
- Biographical identity contains your interactions with society as recorded in public and private databases.
- Biometric identity includes your unique physical attributes such as voiceprint, fingerprint, facial geometry, and iris pattern.

In recent times, the user/password details of millions of individuals have been made public, presenting a substantial risk, especially for students and teachers who often use the same authentication credentials across multiple services. In addition to the traditional user/password combination, alternatives like face recognition, fingerprint validation, and security devices or keys can enhance authentication security [9].

Surveillance entails observing and tracking behaviors, activities, or unusual patterns to direct, safeguard, control, or influence them [10],[11]. Human facial characteristics and behavioral cues are indispensable markers of personal identity. Visual data—predominantly harvested from surveillance video—provides the evidentiary backbone for such recognition and can be scrutinized either in real time or retrospectively for forensic review .Within this domain, facial-recognition systems stand out for their versatility: they not only isolate distinctive facial features but also model head-pose dynamics, enabling the prediction of behavioral intent. When integrated with motion-detection algorithms, these systems form a robust framework for confirming identity, continuously auditing an individual's presence or absence, and delivering reliable authentication across a wide spectrum of applications [12],[13].

An essential responsibility for both developers and users of e-learning platforms is to integrate automated monitoring tools to ensure robust monitoring and control during assessments. Since many early e-learning systems lacked built-in proctoring features, there has been an increasing need for supplementary modules that can be integrated into existing Learning Management Systems (LMS) or remote learning platforms. These tools are critical for maintaining academic integrity, offering functionalities such as identity verification, activity surveillance, browser restriction, and real-time or AI-supported invigilation. Integration can be achieved through official plugins or custom development using APIs. By incorporating these tools, the reliability of online examinations is significantly enhanced, fostering greater trust in the e-learning process [14].

The shift to online education has made it difficult to maintain academic integrity, as traditional supervision methods are ineffective for remote exams. Existing tools often fail to detect real-time or subtle cheating. This study proposes an advanced software system using technologies like facial recognition and voice monitoring to identify and prevent academic dishonesty, ensuring fair and credible online assessments.

The rest of the paper is structured as follows: Section 2 defines the research problem. Section 3 outlines the research objectives. Section 4 presents the research methodology. Section 5 provides a literature review. Section 6 presents the materials and methodology. Section 7 discusses the research results. Section 8 outlines the conclusions and future work.

2. STUDY PROBLEM

During the instruction of first-year Computer Department students, a notable disparity was observed between student performance on traditional paper-based examinations and those conducted via the Mansoura University online learning platform. Specifically, students consistently achieved higher scores in the online format, prompting concerns regarding the validity and integrity of remote assessments.

To investigate this disparity, a series of semi-structured interviews were administered to a representative cohort of students. The primary objective was to examine the underlying factors influencing performance variations across different assessment modalities. The qualitative data revealed a troubling pattern: a substantial number of students candidly admitted that the relative ease of cheating during online exams substantially contributed to their elevated scores. The lack of physical supervision and the inherent limitations of conventional online examination platforms were identified as critical enabling factors facilitating academic dishonesty. In response to these findings, the research problem was articulated through the following key questions:

1. *How can the development of the Real Time Online Exam Monitor Management System be applied In Educational Institutions?*
2. *What is the effectiveness of the Real Time Online Exam Monitor Management System in Educational Institutions?*

3. STUDY OBJECTIVES

The primary objectives of this research are to:

- Ensure Fair and Equitable Assessments: Real-time monitoring guarantees that all examinees are evaluated under the same conditions, creating a level playing field.
- Enable Accurate Evaluation of Abilities: By preventing academic dishonesty, the system ensures that exam results accurately reflect students' true knowledge and skills.
- Provide Comprehensive Reporting: Detailed reports generated for each exam session facilitate post-exam review and analysis.
- Support Data-Driven Improvement: Data collected during assessments inform future exam design improvements and help identify areas where students may need additional support.
- Promote Secure Online Testing: The real-time monitoring software equips educational institutions with robust anti-cheating mechanisms to uphold the integrity of online examinations.

4. STUDY APPROACH

The current study employed a descriptive methodology to conduct a comprehensive review and synthesis of existing literature pertinent to the research topic, thereby establishing a solid theoretical foundation. In parallel, an experimental approach was utilized to empirically evaluate the performance and effectiveness of the proposed system in authentic application contexts, specifically focusing on its ability to detect and deter academic dishonesty in online examination environments.

5. LITERATURE REVIEW

Educational institutions have increasingly turned to digital platforms for student engagement, yet many still depend on simple login credentials, leaving eLearning systems vulnerable to fraud and security breaches. The widespread use of online exams has also led to a rise in academic dishonesty, such as impersonation and unauthorized collaboration, mainly due to the absence of physical supervision. These challenges compromise the credibility of assessments and academic qualifications. To address these issues, this study reviews key prior research, providing a foundation for developing more secure and reliable digital assessment solutions.

Barker, T., & Lee, S. (2007), developed an identity verification system that leverages biometric technologies and video communication tools to support remote learning environments, with a focus on ease of use and effectiveness in verifying student identities during online assessments. In the initial phase, the study explored the use of fingerprint recognition through the Microsoft Fingerprint Reader, which proved to be easy to install—an essential feature for distance learners. The registration process was guided by a user-friendly wizard, allowing users to select their preferred hand and finger, with each finger requiring four successful scans. Users could register up to ten fingers and had the option to add more later. In the subsequent phase, the study focused on creating an online identity verification system that incorporates video conferencing, a database of user verification data, and live chat functionality. Given the widespread use of video technology in educational settings, the system aimed to integrate webcam streaming and chat features to provide a reliable and accessible method for verifying the identity of exam candidates in virtual environments.

Senthil Kumar, T., Narmatha, G. (2016), proposed a system for detecting uncommon behavior in lecture halls. The framework consists of three components working together to monitor student behavior during exams. First, the system identifies the student's facial region, then tracks hand movements and related signals. Modern proctoring systems leverage advanced multimedia technologies that are integral to distance learning environments. These systems typically function by having users log in through a browser, where identity verification is conducted automatically. Throughout the knowledge assessment process, the system continuously gathers data from multiple sources, including the user's microphone, webcam, and occasionally the computer screen. Based on this data, the system can autonomously enforce security measures, such as denying access to the test or exam if the person detected via the webcam does not match the registered individual or if any exam protocols are breached. Furthermore, all collected data is made available for review by the examiner, who retains the authority to make the final determination regarding the assessment's validity.

Karakaş, E., Öztozlu, İ., & Erol, V. (2017), explored modern two-factor authentication methods tailored for the online education sector. It notes a trend towards behavioral biometrics, such as cognitive processes and reading patterns, in the two-step verification process. The study recommends utilizing individuals' unique characteristics to enhance security and prevent unauthorized access. By employing camera and audio inputs, authentication can be uniquely verified through simultaneous monitoring of facial expressions, speech patterns, and sound movements. While this approach offers enhanced security compared to existing systems, challenges such as ensuring adequate internet bandwidth and computing power need to be addressed.

Aubin, V., & Mora, M. (2017), presented a new method for verifying individuals' identities by analyzing handwritten text. The proposed present analyzes the writing pressure pattern within grayscale images of handwritten strokes, focusing specifically on the relative positions of the lowest gray value points within the stroke. An image repository comprising 15,000 images from 50 individuals, each contributing 50 samples of 6 different symbols, was established for experimentation. Identity verification utilized a supervised classifier, namely a Support Vector Machine, trained on non-linearly separable data, resulting in the training of 50 classifiers. Positive assessment outcomes revealed an average hit rate surpassing 95% for identity verification across the six analyzed symbols. This method underscores the processing of exceedingly simple characters, which are notably less complex than signatures.

Bawarith, R., Basuhail, A., Fattouh, A., & Gamalel-Din, S. (2017), investigated methods to combat cheating in online exams by introducing ongoing authentication and online proctoring techniques. It proposes an e-exam administration system that uses a fingerprint reader for initial authentication and an Eye Tribe Tracker to ensure the examinee's identity throughout the exam. The system classifies examinee behavior as "cheating" or "non-cheating" based on two key factors: total time spent off-screen and the frequency of off-screen occurrences. Experimental tests demonstrated high effectiveness.

Ramzan, S., Sanjay, K. P., Al Tajiba, Shoeb, S., & D'Souza, K. J. (2019), developed a web-based system to automate the scheduling of invigilation duties and classroom assignments, aiming to improve efficiency and reduce administrative workload. Using intelligent algorithms, the system effectively handled complex constraints and delivered accurate, reliable schedules. Testing confirmed its user-friendliness, stability, and suitability for educational institutions' exam management needs.

Escobar-Grisales, D., Vásquez-Correa, J. C., Vargas-Bonilla, J. F., & Orozco-Arroyave, J. R. (2020), provided a methodology for confirming the identities of students based on their keystroke dynamics (KD). The method is tested in two modes: intrusive and non-intrusive. In the intrusive mode, subjects are aware of the verification process, while in the non-intrusive mode, subjects are unaware and undergo a different writing task for identity confirmation. Features extracted from these tasks are used to construct Gaussian Mixture Models (GMM), which are then compared using probabilistic distances to determine user validity. Unlike other methods in the literature, this approach relies on probabilistic models rather than directly comparing feature sets. The findings show the ability to detect intruders with up to 89% accuracy, as measured by the Equal Error Rate (EER).

Qi, G., Hu, G., Wang, X., Mazur, N., Zhu, Z., & Haner, M. (2021), proposed a framework called EXAM (EXtreme And Moderate feature embeddings), a novel and robust framework for person re-identification (Re-ID) that leverages discriminative feature learning guided by attention mechanisms.

The approach distinguishes between two key types of visual features: “Extreme” features, which highlight unique and highly salient aspects of a person’s appearance, and “Moderate” features, which capture more common and consistent traits. These are extracted through global max-pooling and mean-pooling operations, respectively. The framework employs a multi-loss strategy, combining triplet and cross-entropy loss functions to jointly supervise the learning process. A core strength of EXAM lies in its ability to integrate attention inference from learned embeddings with feature discrimination in an end-to-end training pipeline, where both processes reinforce each other. Through extensive comparative experiments and ablation studies, the effectiveness of EXAM is validated, with results showing that it achieves state-of-the-art performance in challenging Re-ID scenarios.

González Arrieta, A., López Sánchez, D., Sánchez Lázaro, Á. L., Pérez Lancho, M. B., García-Bermejo-Giner, J. R., Hernández Simón, J. A., & Vega Cruz, P. I.(2021), presented an attempt to make users aware of the need to use more advanced secure authentication methods, as traditional methods such as passwords are not secure enough. A second goal is to find out the actual degree of usage of Latch in the community. This study involved 63 students from the Computer Department and 54 staff members of the Science Faculty at the University of Salamanca. It was conducted shortly before the COVID outbreak. The study focused on reviewing the authentication methods used by users when accessing the university's digital services. Specifically, it offered community members participating in the study a second factor of authentication called Latch.

Sahane, S. N., Khapare, M. V., Dughad, S. S., Ambekar, A. R., & Sonawane, V. A. (2024), studied and agreed on the importance of automating the exam hall and seat allocation process to replace the inefficient and error-prone manual methods. They highlight that such a system reduces administrative workload, improves accuracy, and ensures fair and transparent allocation of rooms and invigilation duties. They emphasize the use of a centralized database for reliable data management and the need for accessibility across desktop and mobile devices. Additionally, they recognize the system's ability to support faculty management and adapt to the growing scale of educational institutions, ultimately enhancing overall efficiency and user satisfaction.

Vijaypriya, V., Dhanesh, P. M., Giridhar, V., & Harish, B. L. (2024), outlined proctoring system enhances exam security and integrity by utilizing advanced technologies to remotely monitor students. It analyzes gaze movements, facial features, and mouth activity to discover probable cheating, such as using unauthorized materials or verbal communication. In addition, the system utilizes the YOLO algorithm for real-time detection of prohibited substances, such as phones and books. This automated monitoring allows for immediate identification of suspicious behavior and timely intervention, ensuring fair and reliable online assessments.

Narayana, K. L., Dinesh, G., Kumar, K. K., Adithya, P. P., Sai, M. H. V. S., & Reddy, V. C. M. (2025), developed and tested an online exam proctoring system to ensure secure, real-time performance and effective AI-based monitoring. Key features such as user authentication, exam creation, access control, and live proctoring were successfully implemented. Examiners could create and manage exams, while students accessed them with granted permission. The AI proctoring module reliably detected cheating behaviors, such as multiple persons, mobile phone use, tab switching, and gaze deviation, and automatically submitted exams after repeated violations. Real-time testing confirmed the system’s reliability and effectiveness in maintaining exam integrity.

6. MATERIALS AND METHODS

Recognizing the urgent need to uphold academic standards and ensure fairness in assessment, we designed and developed an advanced solution: the Real-Time Online Exam Monitor Management System. This system is specifically tailored for educational institutions seeking to enhance the integrity of online examinations .The proposed system integrates cutting-edge monitoring technologies, including facial recognition for identity verification, voice analysis for detecting background conversations, screen activity tracking, and object detection to identify unauthorized materials or devices. By enabling real-time surveillance using students’ mobile devices, the system provides a proactive approach to mitigating cheating and reinforces accountability during remote assessments .In doing so, the system not only strengthens the credibility of online exams but also supports a more accurate and equitable evaluation of student learning outcomes. The subsequent sections detail the system's development methodology, technical architecture, and implementation framework.

6.1 System Development Stages

- **Requirements Analysis**

The initial phase focused on understanding the core needs of educational institutions to ensure secure and fair online exams. Major concerns identified included impersonation, use of unauthorized materials, and lack of supervision, all of which compromise the integrity of remote assessments.

- **System Design**

The system was designed with real-time monitoring features to address these issues. The system incorporated key technologies such as:

- ✓ Facial Recognition for identity verification.
- ✓ Voice Analysis to detect background conversations.
- ✓ Behavioral Monitoring to track on-screen activity.

These technologies were selected to create a secure and scalable monitoring framework.

- **System Development**

The system was built using a modular architecture and integrated with multiple monitoring tools, including:

- ✓ Real-time video recording.
- ✓ Facial and voice recognition.
- ✓ Screen activity tracking.
- ✓ Object detection for unauthorized materials.

Together, these components form a comprehensive solution for maintaining academic integrity in online examinations. Figure 1 presents a diagram illustrating the Real-Time Online Exam Monitoring System, which outlines the operational framework of a Monitor Management System designed for online examinations or remote assessments.

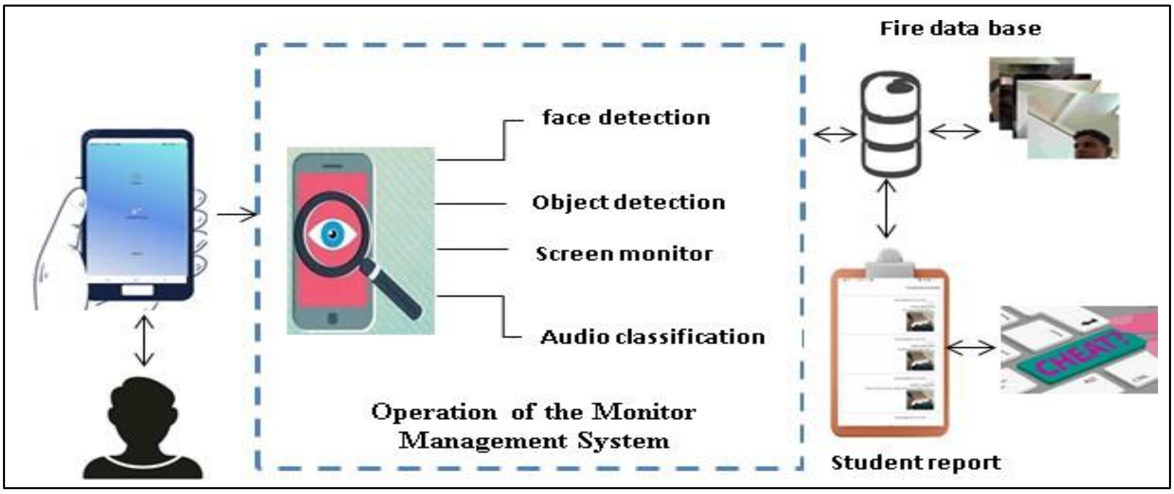


Figure 1. The Proposed Examination Monitoring Management System

The diagram displays a clear representation of the system's components and their interactions during the examination process. Below is a detailed breakdown of the core components and workflow used:

❖ ***User Device Interaction***

A student uses a mobile device (like a smartphone or tablet) during an online exam. The device acts as a monitoring tool while the student is being assessed.

❖ *Monitoring System Functions*

Inside the dashed box, the Monitor Management System performs several surveillance tasks using the mobile device's sensors (camera, microphone, etc.), as shown in Figure 2.

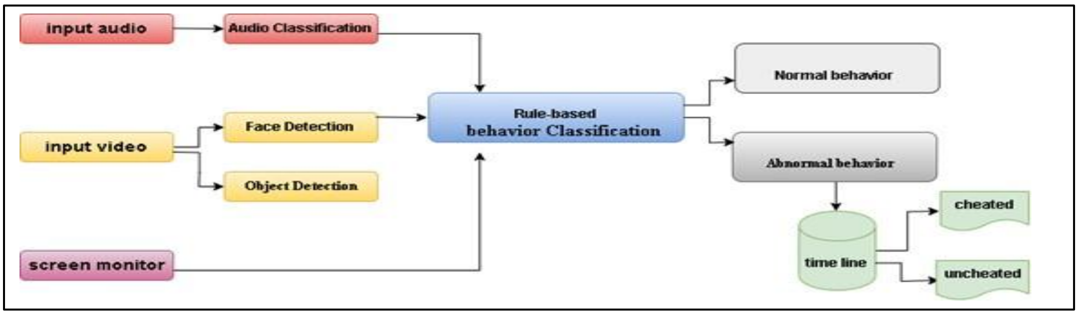


Figure 2. Student Behavior and Monitoring System Functions Analysis

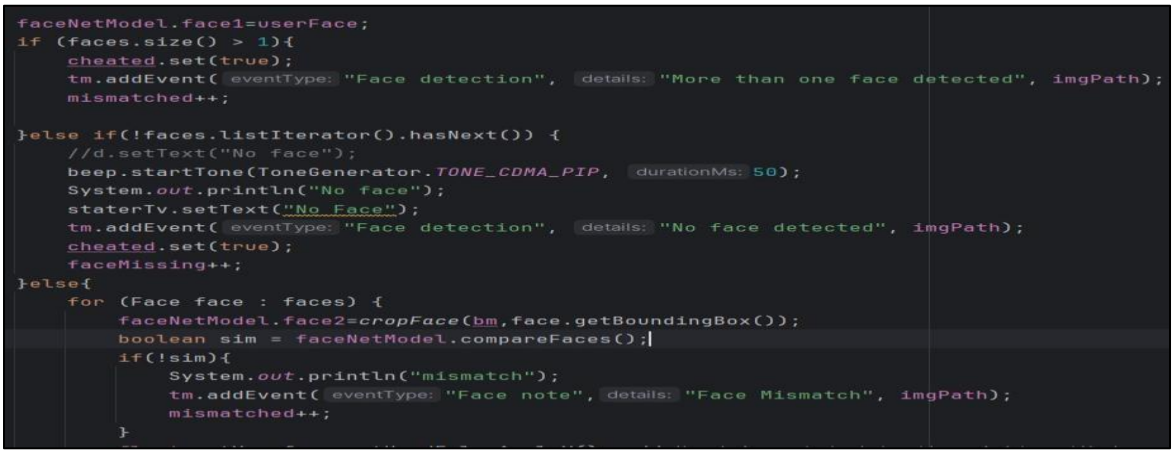
Below is a breakdown of the basic components and workflow involved in the Figure above:

1) Face Detection

Identifies the presence and identity of the student to ensure they are the only one present using ML Kit, TensorFlow Lite models, and the FaceNet model. Steps for Face Detection below:

- ✓ Start by capturing an input image frame.
- ✓ ML Kit's face detection, face contour detection) for face verification.
- ✓ Using the FaceNet model to match with the original image from Firebase.
- ✓ Output results: store the results) :no face or, more than one face or face mismatch).

A snippet of the comparison process in Face Detection is shown in Figure 3.



```
faceNetModel.face1=userFace;
if (faces.size() > 1){
    cheated.set(true);
    tm.addEvent( eventType: "Face detection",  details: "More than one face detected", imgPath);
    mismatched++;

}else if(!faces.listIterator().hasNext()) {
    //d.setText("No face");
    beep.startTone(ToneGenerator.TONE_CDMA_PIP,  durationMs: 50);
    System.out.println("No face");
    staterTv.setText("No Face");
    tm.addEvent( eventType: "Face detection",  details: "No face detected", imgPath);
    cheated.set(true);
    faceMissing++;
}else{
    for (Face face : faces) {
        faceNetModel.face2=cropFace(bm,face.getBoundingBox());
        boolean sim = faceNetModel.compareFaces();
        if(!sim){
            System.out.println("mismatch");
            tm.addEvent( eventType: "Face note", details: "Face Mismatch", imgPath);
            mismatched++;
        }
```

Figure 3. Comparison Process in Face Detection

2) Object Detection

Detects suspicious objects like additional devices, books, or unauthorized notes. These steps will be explained below.

- ✓ Input Data: Capture input image frame.
- ✓ Preprocessing: Using ML Kit's image labeling.
- ✓ Image labeling: Used to identify general objects.
- ✓ Log detected objects and metadata (e.g., paper, mobile, book, hand).

✓ Output results: Used to store the results of abnormal behavior.

Figure 4 shows a flowchart explaining the mechanism of the proposed system in face detection and object detection.

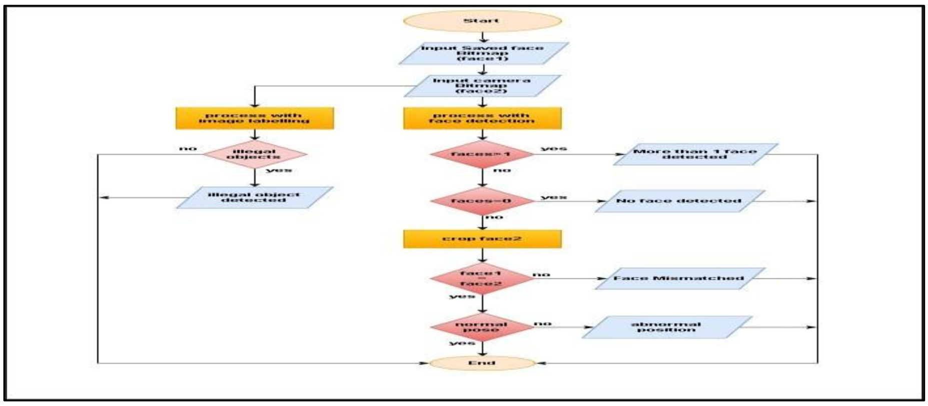


Figure 4. Steps of Face Detection and Object Detection

3) *Audio Classification*

Analyzes surrounding sounds to detect human speech or background conversations that may indicate cheating. Steps for Audio Classification.

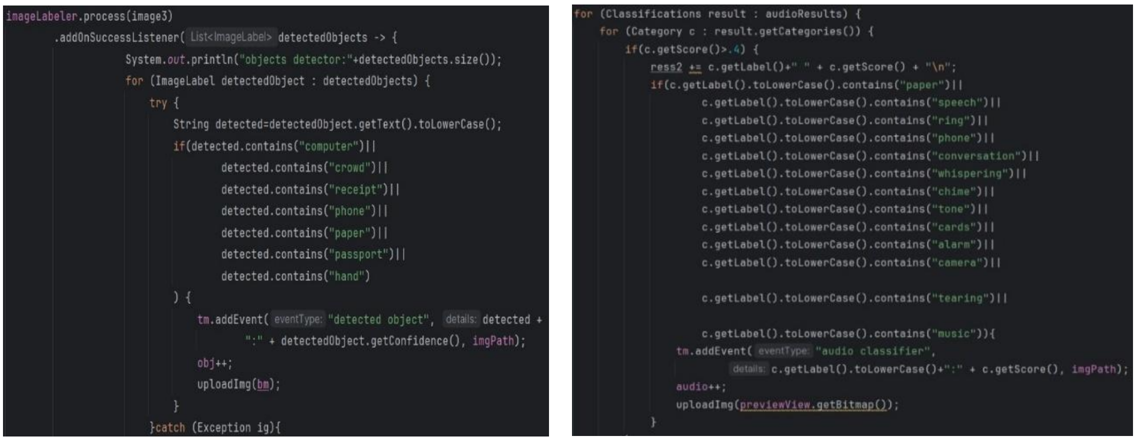
- Input audio: Capture audio from the microphone.
- Model input preparation: Convert the recorded audio to fit the tensor audio type.
- Classification: Includes the following:

- Use a pre-trained or custom-trained model to classify the audio.
- Convolutional Neural Networks (CNNs) using TensorFlow.

- Sound classification with YAMNet.
- Output results: Includes the following:

- Display the predicted class (e.g., speech, ring, tone, alarm, paper).
- Abnormal sound.

Figure 5(a, b) displays a code snippet that demonstrates detected objects and audio classification.



```
imageLabeler.process(image3)
        .addOnSuccessListener( List<ImageLabel> detectedObjects -> {
                System.out.println("objects detector:"+detectedObjects.size());
                for (ImageLabel detectedObject : detectedObjects) {
                    try {
                        String detected=detectedObject.getText().toLowerCase();
                        if(detected.contains("computer")||
                                detected.contains("crowd")||
                                detected.contains("receipt")||
                                detected.contains("phone")||
                                detected.contains("paper")||
                                detected.contains("passport")||
                                detected.contains("hand")
                        ) {
                            tm.addEvent( eventType: "detected object",  details: detected +
                                    ":" + detectedObject.getConfidence(), imgPath);
                            obj++;
                            uploadImg(bm);
                        }
                    }catch (Exception ig){
```

(a)

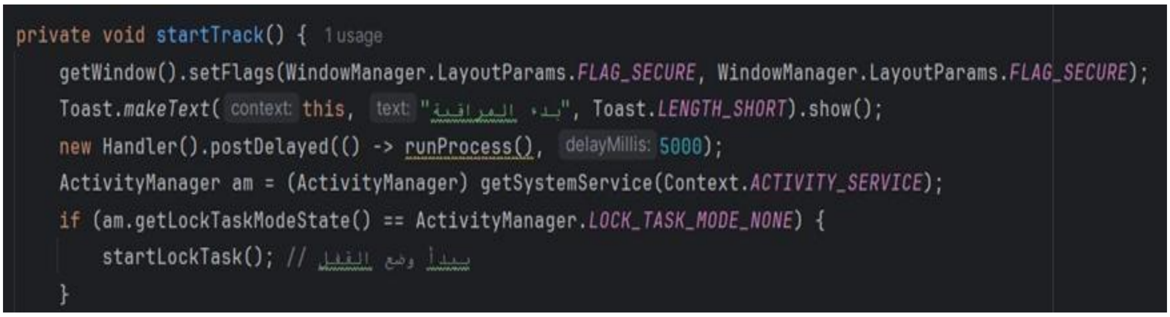
```
for (Classifications result : audioResults) {
    for (Category c : result.getCategories()) {
        if(c.getScore()>.4) {
            ress2 += c.getLabel()+" " + c.getScore() + "\n";
            if(c.getLabel().toLowerCase().contains("paper")||
                    c.getLabel().toLowerCase().contains("speech")||
                    c.getLabel().toLowerCase().contains("ring")||
                    c.getLabel().toLowerCase().contains("phone")||
                    c.getLabel().toLowerCase().contains("conversation")||
                    c.getLabel().toLowerCase().contains("whispering")||
                    c.getLabel().toLowerCase().contains("chime")||
                    c.getLabel().toLowerCase().contains("tone")||
                    c.getLabel().toLowerCase().contains("cards")||
                    c.getLabel().toLowerCase().contains("alarm")||
                    c.getLabel().toLowerCase().contains("camera")||

                    c.getLabel().toLowerCase().contains("tearing")||

                    c.getLabel().toLowerCase().contains("music")){
                tm.addEvent( eventType: "audio classifier",
                         details: c.getLabel().toLowerCase()+":" + c.getScore(), imgPath);
                audio++;
                uploadImg(previewView.getBitmap());
            }
```

(b)

Figure 5. (a) Code Snippet Showing Detected Objects, (b) Audio Classification

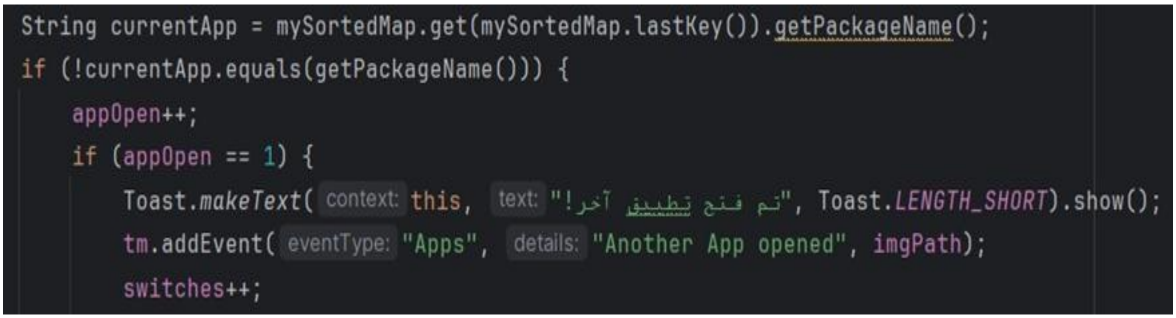
4) Screen Monitor

Tracks the usage of the screen to prevent switching between apps or accessing restricted materials. At the beginning of the exam, the system activates its monitoring protocol and secures the screen environment by restricting access to unauthorized applications and system functions (Figure 6). This mechanism ensures that students remain confined to the designated exam interface for the duration of the session, minimizing opportunities for academic misconduct. As the exam progresses, the system continuously monitors the student's screen activity in real time. It is specifically designed to detect any attempts to launch unauthorized applications or open multiple active windows, thereby preserving the integrity of the testing environment. Upon detecting such behavior, the system immediately issues a warning through a combination of a visual notification and an audible alert, prompting the student to return to the exam interface and remain focused (Figure 7).



```
private void startTrack() {  1 usage
    getWindow().setFlags(WindowManager.LayoutParams.FLAG_SECURE, WindowManager.LayoutParams.FLAG_SECURE);
    Toast.makeText( context: this,  text: "بدء المراقبة", Toast.LENGTH_SHORT).show();
    new Handler().postDelayed(() -> runProcess(),  delayMillis: 5000);
    ActivityManager am = (ActivityManager) getSystemService(Context.ACTIVITY_SERVICE);
    if (am.getLockTaskModeState() == ActivityManager.LOCK_TASK_MODE_NONE) {
        startLockTask(); // يبدأ وضع القفل
    }
```

Figure 6. Code Snippet Opens a Lot of Applications



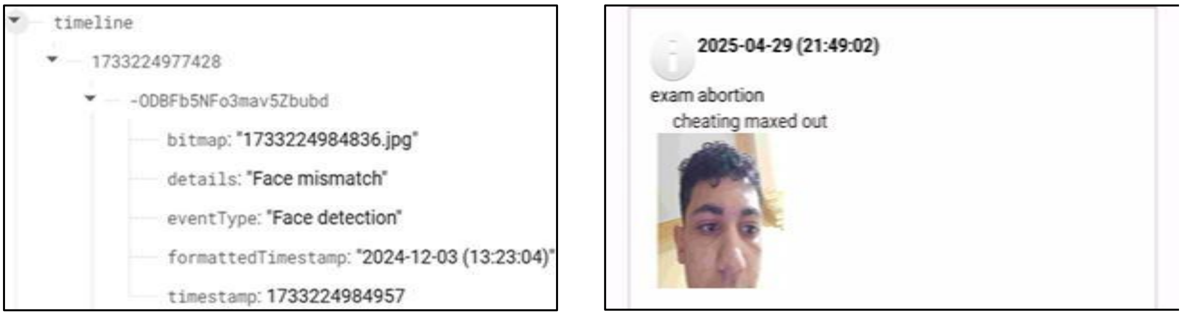
```
String currentApp = mySortedMap.get(mySortedMap.lastKey()).getPackageName();
if (!currentApp.equals(getPackageName())) {
    appOpen++;
    if (appOpen == 1) {
        Toast.makeText( context: this,  text: "تم فتح تطبيق آخر!", Toast.LENGTH_SHORT).show();
        tm.addEvent( eventType: "Apps",  details: "Another App opened", imgPath);
        switches++;
```

Figure 7. Code Snippet Initiates Monitoring and Locks the Screen

❖ *Data Processing and Reporting*

- The monitoring data is sent to a Firebase database (Firebase database) for real-time storage and analysis.
- From there, a student report is generated, which includes:

- Visual evidence (photos or videos).
- Detected anomalies or cheating behaviors.
- A decision or flag indicating potential cheating. Figure 8(a),(b) display the real-time database and timeline event.



```
timeline
    1733224977428
        -ODBFb5NFo3mav5Zbubd
            bitmap: "1733224984836.jpg"
            details: "Face mismatch"
            eventType: "Face detection"
            formattedTimestamp: "2024-12-03 (13:23:04)"
            timestamp: 1733224984957
```

2025-04-29 (21:49:02)
exam abortion
cheating maxed out

(a) (b)

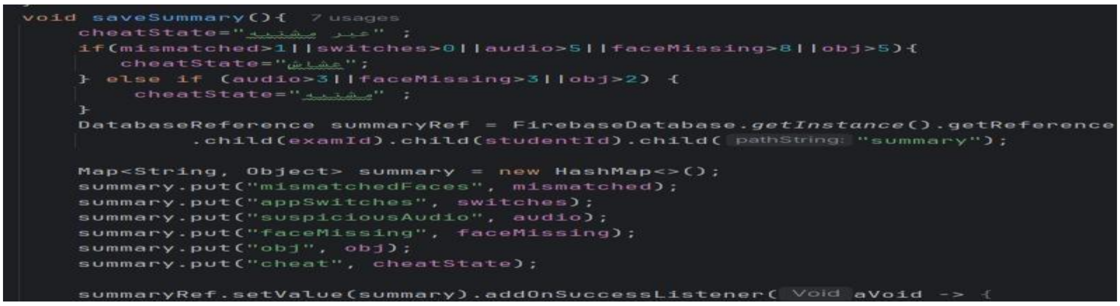
Figure 8. (a) Snippet of Real-Time Database, (b) Cheating Maxed Out

❖ ***Cheat Detection Outcome***

If any suspicious behavior, such as suspected cheating or a confirmed violation, is detected, the system immediately flags the incident in real time and generates a detailed report. As below, student report in pseudo code:

```
// Initialize result as "Not suspected"

Result = "Not suspected"

// Check for suspicious conditions

IF detected_objects > 2 OR face_missing > 3 OR suspicion_audio > 3 THEN

Result = "Suspicion of cheating"

ELSE IF face_mismatching = TRUE OR app_switch = TRUE OR detected_objects > 5 OR
face_missing > 5 OR suspicion_audio > 5 THEN

Result = "Cheater"

END IF
```

This report includes key evidence like video snapshots, audio cues, and screen activity logs, and the incident is recorded in the student's exam results. Human invigilators can review the report for further evaluation, promoting fairness, transparency, and accountability in online assessments. Figure 9 displays the Cheat Detection Outcome Code snippet.

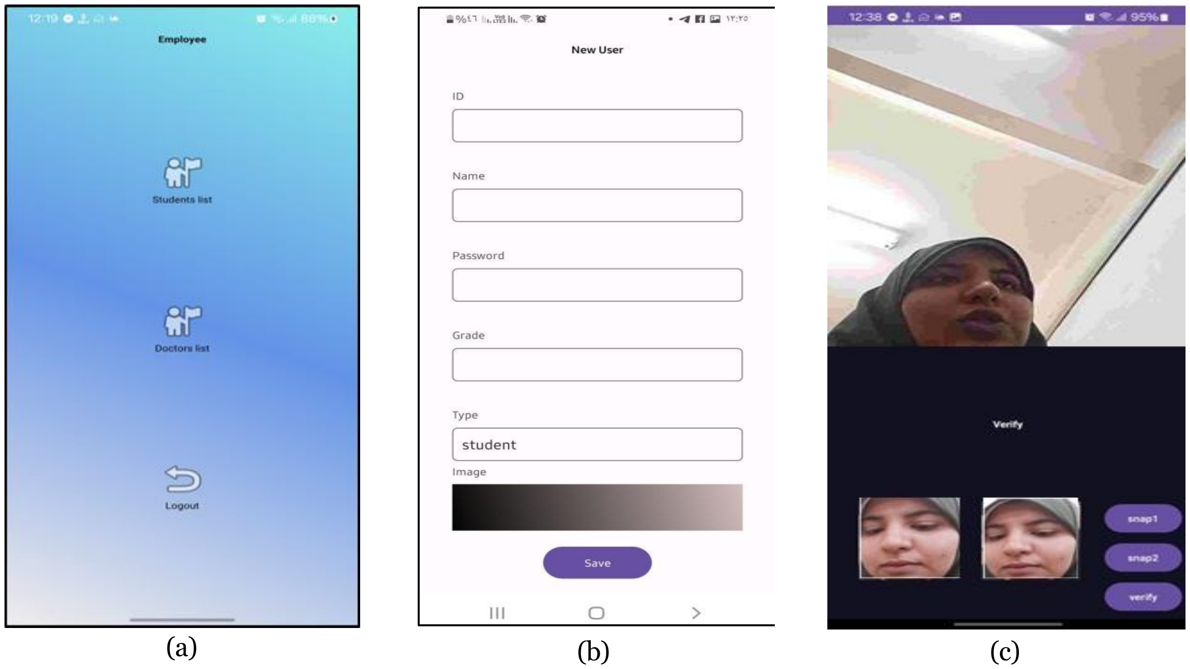


```
void saveSummary(){  7 usages
    cheatState="غير مشتبه" ;
    if(mismatched>1||switches>0||audio>5||faceMissing>8||obj>5){
        cheatState="غشاش";
    } else if (audio>3||faceMissing>3||obj>2) {
        cheatState="مشتبه" ;
    }
    DatabaseReference summaryRef = FirebaseDatabase.getInstance().getReference
            .child(examId).child(studentId).child( pathString: "summary");

    Map<String, Object> summary = new HashMap<>();
    summary.put("mismatchedFaces", mismatched);
    summary.put("appSwitches", switches);
    summary.put("suspiciousAudio", audio);
    summary.put("faceMissing", faceMissing);
    summary.put("obj", obj);
    summary.put("cheat", cheatState);

    summaryRef.setValue(summary).addOnSuccessListener( Void aVoid -> {
```

Figure 9. Cheat Detection Outcome

- ## Authentication phase

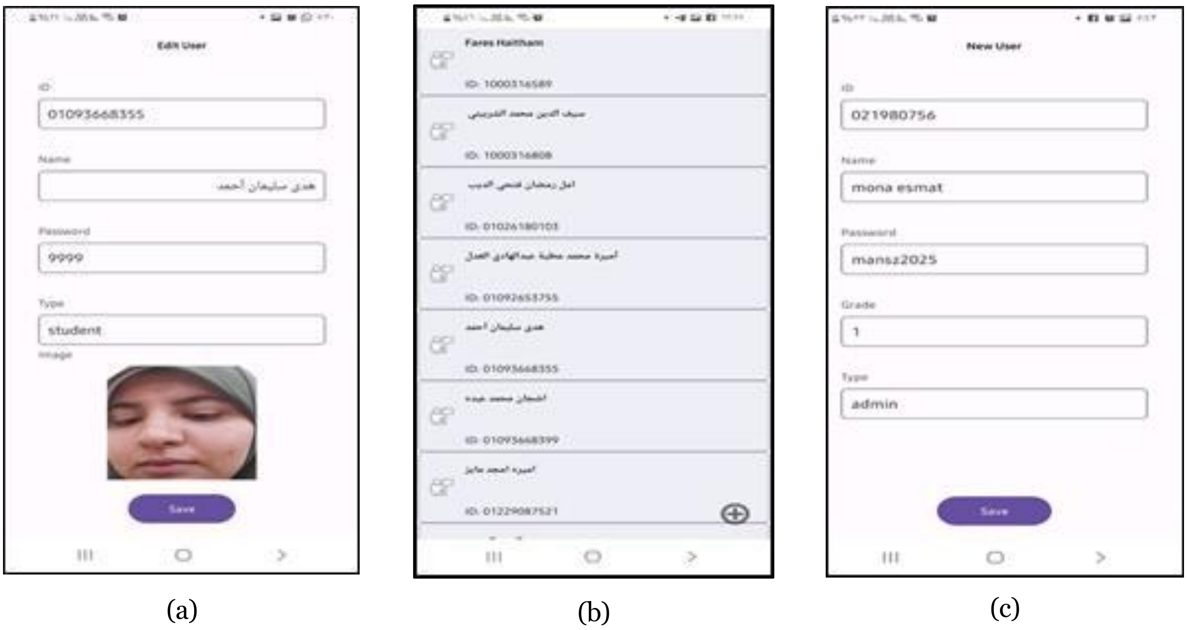
To ensure the integrity of internet based examinations, the system employs a multi-layered identity verification protocol that must be completed before a student is granted access to the exam. This verification relies on the student's pre-registered credentials, securely stored within the system's encrypted database, ensuring that only the legitimate candidate is permitted to initiate and complete the examination. Administrators are provided with a dedicated management interface to pre-register students according to their academic year or course group. During this registration process, each student is issued a unique login ID and password, and a facial image is captured via the application. This biometric data is later utilized during the exam session for real-time facial recognition, allowing the system to authenticate the student's identity continuously and at multiple checkpoints. This comprehensive approach not only deters impersonation but also strengthens trust in the fairness and credibility of the online examination environment. Figure 10 (a) displays the Main interface for registering an employee, and (b), (c) displays the Student registration screen for entering personal, academic information, and the student’s picture.



(a) (b) (c)

Figure 10. (a) Main Interface for Registering an Employee, (b) Student Registration Screen for Entering Personal and Academic Information, Image Capture Screen Displayed when the Admin Taps the Photo Area to Take a Student’s Picture, (c) Face Verification Screen Showing Snap 1 and Snap 2 Followed by the Verification.

Figure 11 showcases three key user interface screens within the system. Subfigure (a) displays the Student Information Screen, presenting detailed academic and personal data for each student. Subfigure (b) illustrates the Student List View, offering a centralized overview of all registered students to support efficient data management. Subfigure (c) features the Course Instructor Registration Screen, allowing instructors to enter their details and register for multiple course exams across different academic years, ensuring accurate mapping between instructors and their assigned examinations



Edit User

ID
01093668355

Name
هدى سليمان أحمد

Password
9999

Type
student

Image

(a)

Fares Haitham
ID: 1000316589

سيف الدين محمد الشربيني
ID: 1000316808

امل رمضان فتحي الديب
ID: 01026180103

أميرة محمد عطية عبدالهادي العدل
ID: 01092653755

هدى سليمان احمد
ID: 01093668355

اشجان محمد عبده
ID: 01093668399

اميرة امجد عايز
ID: 01229087521

(b)

New User

ID
021980756

Name
mona esmat

Password
mansz2025

Grade
1

Type
admin

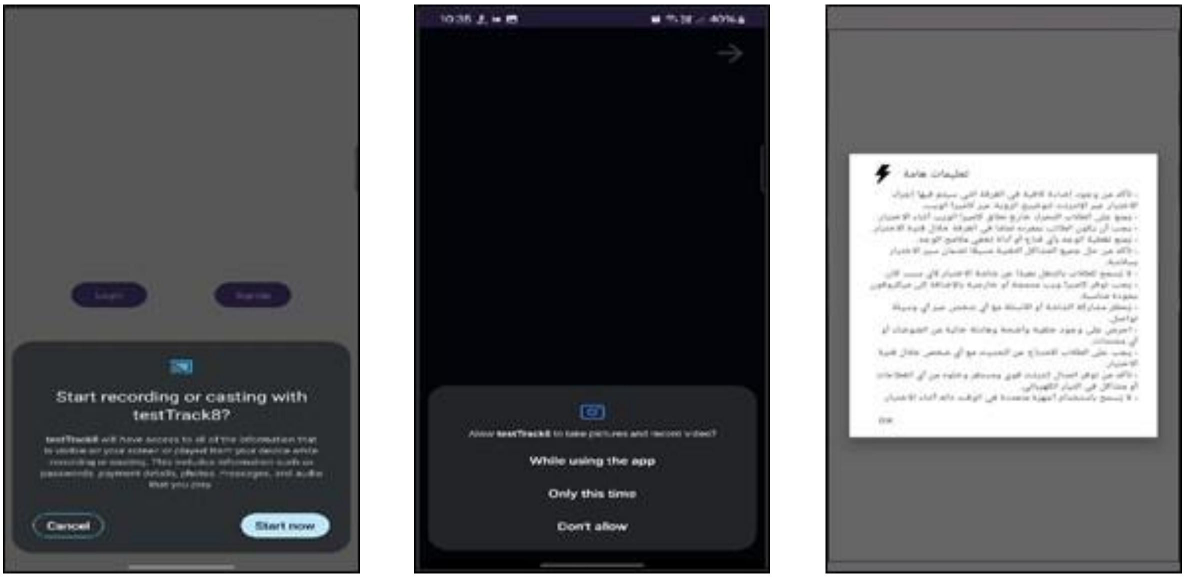
(c)

Figure 11. (a) Student Information Screen Displaying Personal and Academic Details, (b) Student List View Showing All Registered Students in the System, (c) Doctor Registration Screen for Entering Personal Information

▪ Login Phase and Start of Monitoring for Online Exams

The application will request permission to use your camera and microphone before the exam begins. Granting this permission allows us to record students' faces and surroundings during the test. These recordings are used by our system to maintain exam integrity and prevent cheating, ensuring the reliability of online assessments. Testing Environment: Students are required to take the exam in a quiet, well-lit, and distraction-free environment to ensure clear visibility and audibility by the proctoring system. The following conditions must be met:

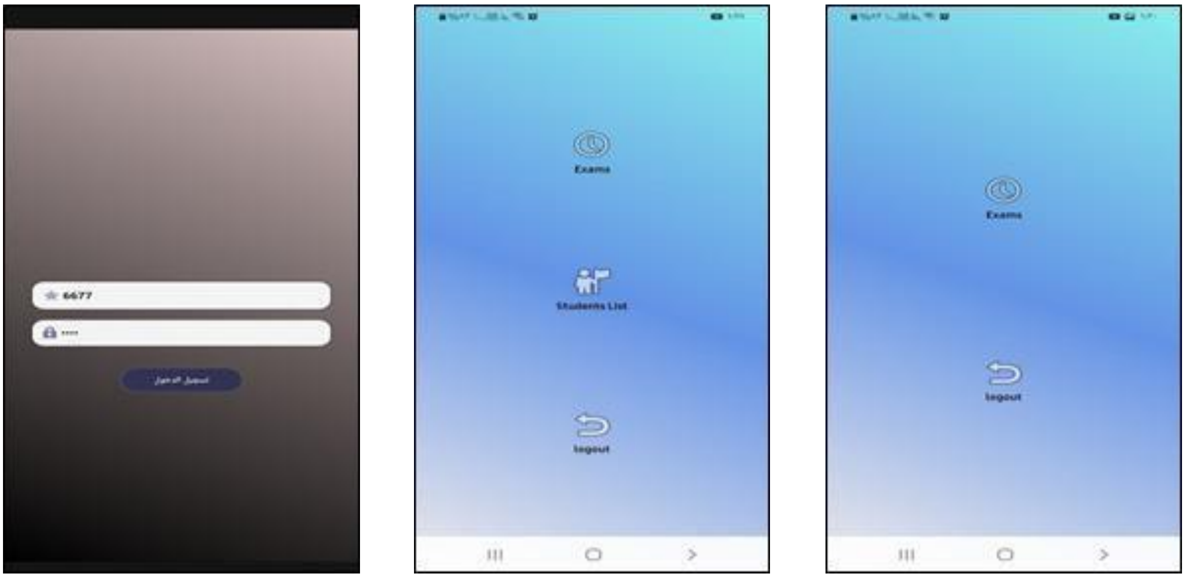
- The testing area must be free of distractions, such as other individuals, televisions, or background music.
- Sufficient lighting must be provided to illuminate the student’s face and the surrounding area.
- Background noise should be kept to a minimum to avoid interference with audio monitoring.
- Make sure the front camera has a clear view of your entire face. As we showed in Figure 12.



(a) (b) (c)

Figure 12. (a), (b) Permission to Use the Camera and Microphone, and (c) Instruction Screen

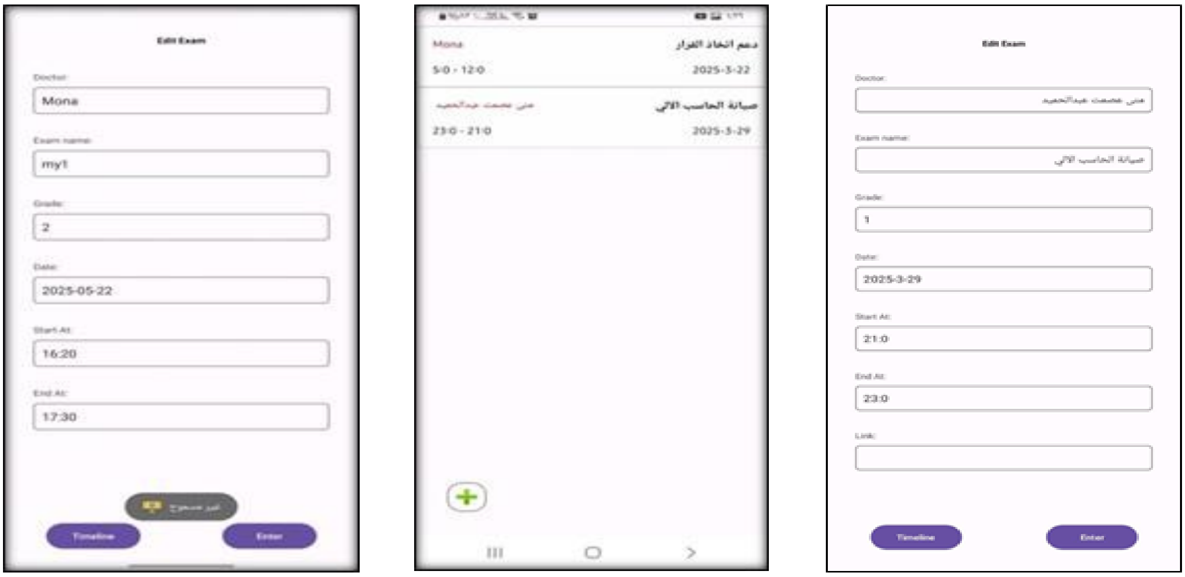
Figure 13 illustrates the design of the mobile application, showcasing both the registration screen and the main user interfaces for students and lecturers. Figure 13(a) depicts the registration process, where users are required to enter a username and password, which will be used for authentication in future sessions. Additionally, Figures 13(b) and 13(c) display the main interfaces tailored for students and lecturers, respectively. The lecturer's interface provides functionalities to create new exams by entering all relevant details, as well as access a comprehensive activity log for each student, capturing all events recorded by the proctoring system. On the other hand, the student's interface displays a list of available exams, which can be accessed only during the designated time slots.



(a) (b) (c)

Figure 13. (a) User Enters His Data and Presses "Login" (b), (c) The Main Screen for Lecture and Student

Figure 14(a) demonstrates that students attempting to access the exam outside the scheduled time receive a notification denying entry. Figure 14(b) illustrates the exam creation process, where lecturers initiate the setup by clicking the "+" icon. This action leads to the form shown in Figure 14(c), where key information such as the lecturer's name, exam title, scheduled date and time, and a direct exam link is entered to finalize the exam setup.



Edit Exam

Doctor: Mona
Exam name: my1
Grade: 2
Date: 2025-05-22
Start At: 16:20
End At: 17:30

غير مسموح

(a)

Mona — دعم اتخاذ القرار
5:0 - 12:0 — 2025-3-22

منى محمد عبدالحميد — صيانة الحاسب الآلي
23:0 - 21:0 — 2025-3-29

(b)

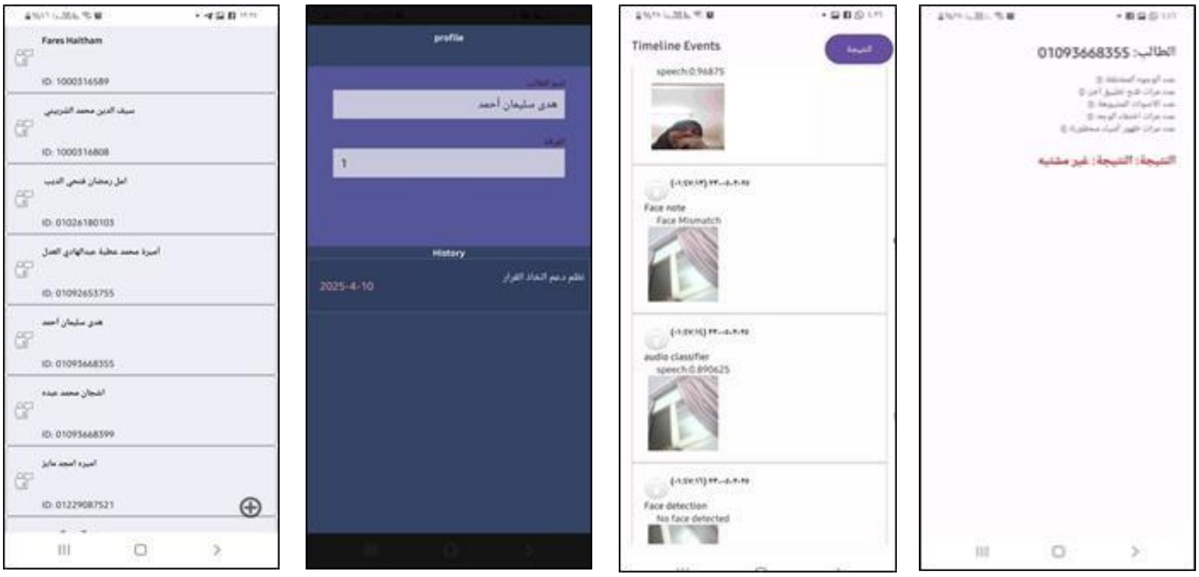
Edit Exam

Doctor: منى محمد عبدالحميد
Exam name: صيانة الحاسب الآلي
Grade: 1
Date: 2025-3-29
Start At: 21:0
End At: 23:0
Link:

(c)

Figure 14. (a) Access to the Exam Outside the Scheduled Time, (b)Insert a New Exam, and (c) Exam Details

Figure 15 showcases key features of the exam monitoring system: (a) a student list for quick access, (b) individual student profiles with ID and photo, (c) a timeline of recorded exam events highlighting suspicious behavior, and (d) exam results for performance evaluation and integrity verification.



Fares Haitham
ID: 1000316589

سيف الدين محمد الشربيني
ID: 1000316808

امل رمضان فتحي الديب
ID: 01026180103

أميرة محمد عطية عبدالهادي العدل
ID: 01092653755

هدى سليمان احمد
ID: 01093668355

اشجان محمد عبده
ID: 01093668399

اميرة امجد مايز
ID: 01229087521

(a)

profile

اسم الطالب: هدى سليمان أحمد
الفرقة: 1

History

نظم دعم اتخاذ القرار — 2025-4-10

(b)

Timeline Events

speech:0.96875

[illegible]
Face note
Face Mismatch

[illegible]
audio classifier
speech:0.890625

[illegible]
Face detection
No face detected

(c)

الطالب: 01093668355

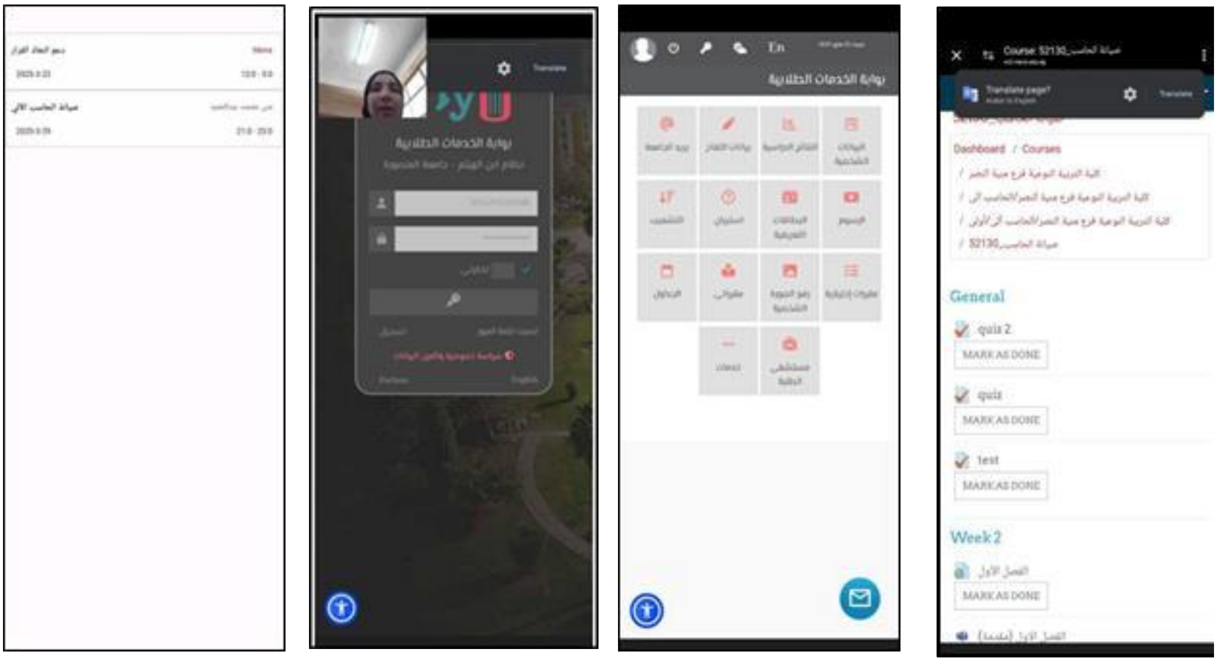
عدد الوجوه المختلفة: 0
عدد مرات فتح تطبيق آخر: 0
عدد الأصوات المشبوهة: 0
عدد مرات اختفاء الوجه: 0
عدد مرات ظهور أشياء محظورة: 0

النتيجة: النتيجة: غير مشتبه

(d)

Figure 15. (a) Students List, (b) Student Profile, (c) Timeline Events, and (d) Student Result

Using the mobile application, the student selects the intended exam from the available list. Then he accesses their account, and the system then automatically redirects the student to the Mansoura University educational platform, simultaneously launching the exam environment and activating the proctoring system as shown in Figure 16. Thus, the system reached its initial version.



(a) (b) (c) (d)

Figure 16. (a) Exams List, (b), (c), (d) Student's Mansoura University Educational Platform Account

6.2 System Testing

- Conducting pilot tests to ensure the system's efficiency in detecting cheating incidents. Figure 17 displays the Exam Monitor Management System in the test stage.
- To verify its validity, it was presented to a panel of five evaluators to assess its efficiency and suitability for operation on the Mansoura University online learning platform. This evaluation was conducted using a specially designed assessment form. The evaluators unanimously agreed on the quality and reliability of the monitoring system, confirming its effectiveness and readiness for implementation.

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/
Research Article

Figure 17. Exam Monitor Management System in Test Stage

- ***Building and Adjusting the Achievement Test:*** To ensure the effectiveness of the Real-Time *Online* Exam Monitor Management System in reducing cheating among first-year Computer Department students. We designed an achievement test for the decision support systems course. An initial achievement test was constructed, consisting of 12 items, and to ensure its validity, it was presented to a group of three reviewers. The reviewers proposed some suggestions, including editing the wording of some items and deleting two items due to their unsuitability for first-year students. Following these changes, the achievement test final version contained ten application-ready elements. The questions were uploaded to the online learning platform of Mansoura University.

- ***The Reliability of the Achievement Test for the Decision Support Systems Course:***The test-retest method was used to determine the achievement test's reliability. A pilot sample of thirty first-year students from Mansoura University's Faculty of Specific Education's Computer Department were given the test. The same sample was given the achievement test again three weeks later. After recording the results and statistically processing them using the Pearson correlation coefficient, the reliability coefficient value was as shown in the following table.

Table 1: Reliability Coefficient of the Achievement Test

Reliability Coefficient	Significance Level
0.736	0.01

Table 1 makes it evident that the achievement test's reliability coefficient for the proposed system as a whole is 0.736, which is significant at (0.01, and this is a good reliability coefficient for this method.

6.3 Selection of the Research Sample

A total of thirty first-year students from Mansoura University's Faculty of Specific Education's Computer Department made up the research sample.

6.4 Selection System Implementation

Implementation (Experimental Study): The research tool (the achievement test) for the decision support systems course was administered to the research sample before the implementation of the monitoring system through the Mansoura University online learning platform, and their scores were recorded. The students (research sample) were then instructed to download the proposed monitoring system the following day, follow the provided guidelines, and access the Mansoura University online learning platform to retake the decision support systems achievement test after installing the system. The students' scores in the post-test were recorded in preparation for statistical analysis.

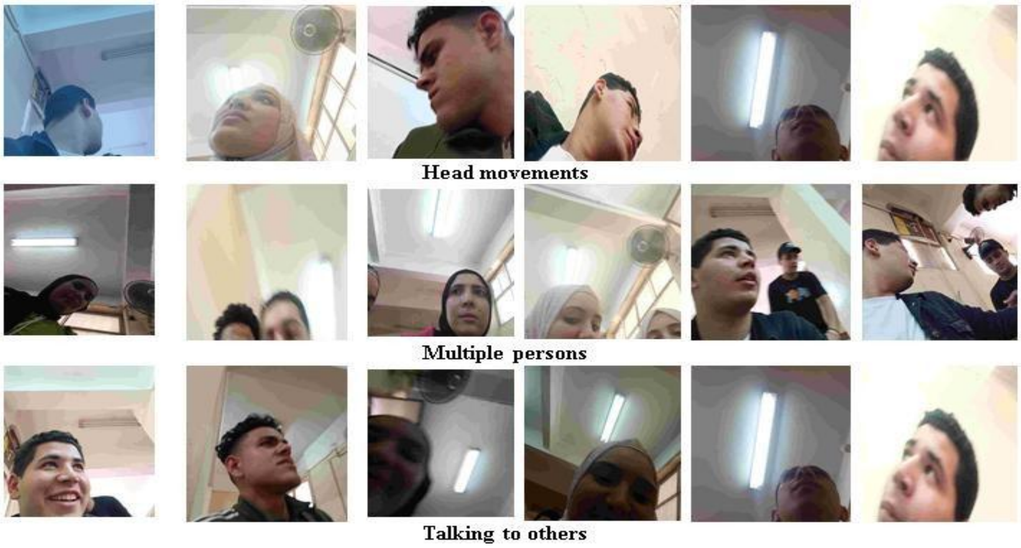


Figure 18. Cheating Activities Detection in Online Exams on the Implementation Stage

Figure 18 highlights the system's real-time detection of cheating behaviors during online exams, such as unusual head movements, the presence of multiple individuals, and conversations during the test. Detected incidents are automatically logged in the student's event record within Firebase, allowing the course instructor to review and take appropriate action. This process enhances exam security and supports timely intervention to uphold academic integrity.

7. RESULTS AND DISCUSSION

In light of the research problem and hypothesis, the data were analyzed as follows.

- ***Testing the Research Hypothesis***

"There is a statistically significant difference at the level of significance (≤0.05) between the mean scores of the students, the research sample on the achievement in the pre- and post-application tests using the Real Time Online Exam Monitor Management System in favor of the pre-application".

To verify the research hypothesis, the t-test for paired samples statistics was used. The mean and standard deviation of the students' scores in the achievement test were calculated for both applications: before using the monitoring system and after using it. The t-value corresponding to the difference between the two means was computed, along with the significance level associated with the t-value. Table 2 presents these results.

Table 2: T-Value and Significance of the Difference between Mean Scores of Students' Research Sample in Pre and Post Applications of the Achievement Test

Test	No of Students	Mean	Std	Degree of Freedom	T Value	Significance Level
Pre	30	8.30	1.62	29	10.31	0.01
Post	30	4.46	1.25			

It is clear from Table 2 the following:

- There is a statistically significant difference at the level of (0.01) between the mean scores of the students, the research sample in the achievement of the pre using the Real Time Online Exam Monitor Management System and post using the Real Time Online Exam Monitor Management System applications in favor of the pre-application.

- The level of the students - the research sample - in the post-application decreased in achievement after using the Real Time Online Exam Monitor Management System compared to their level in the pre-application.
- The dispersion of the scores of the students - the research sample - decreased in achievement after using Real Time Online Exam Monitor Management System, and this indicates a decrease in the level of most students, the proximity of their level, and the homogeneity of the scores they obtained in the achievement after using the Real Time Online Exam Monitor Management System.

These results indicate the achievement of the hypothesis of the research, and the results can be interpreted as follows:

These findings suggest that before implementing the monitoring system, some students may have engaged in dishonest practices, which artificially inflated their scores. However, after introducing the monitoring system, performance levels declined to reflect genuine comprehension, highlighting the importance of secure and integrity-driven online assessments. Additionally, the increased homogeneity in scores underscores the system's role in leveling the playing field, ensuring that all students are evaluated based on merit rather than external factors. These results reinforce the necessity of integrating real-time monitoring solutions in online learning platforms to uphold academic integrity, enhance the credibility of online assessments, and provide a more accurate measure of students' learning outcomes. These results agree with the results of studies by Sinha, P., Dileshwari, & Yadav, A. (2020), Shkodzinsky, O., & Kłos-Witkowska, A. (2023), Vijaypriya, V., Dhanesh, P. M., Giridhar, V., & Harish, B. L. (2024), and Narayana, K. L., Dinesh, G., Kumar, K. K., Adithya, P. P., Sai, M. H. V. S., & Reddy, V. C. M. (2025).

- ***The Effectiveness of Using the Real-Time Online Exam Monitor Management System in Reducing Cheating in Exams among First-Year Computer Department Students***

To measure the effectiveness of using the Real-Time Online Exam Monitor Management System in reducing cheating in exams among first-year computer department students, the t-value and correlation coefficient between the students' scores in the pre- and post-application of the achievement test were calculated, as well and the effect size. Table 3 illustrates this:

Table 3: Effect Size of Using the Real-Time Online Exam Monitor Management System in Reducing Cheating in Exams

T-Value	Correlation Coefficient	Effect Size
10.314	0.014	0.677

It is clear from Table 3 that the effect size is 0.677, which is a large effect size, and this indicates that using the Real-Time Online Exam Monitor Management System is effective in reducing cheating in exams among first-year computer department students. Thus, we have answered the second question of the research questions, which states: "What is the effectiveness of the Real Time Online Exam Monitor Management System in educational institutions?"

8. CONCLUSION AND FUTURE WORK

The transition to online education has introduced significant challenges in preserving academic integrity, particularly during remote assessments. This study identified a clear disparity in student performance between traditional in-person examinations and their online counterparts, largely attributed to the heightened risk of academic dishonesty in the absence of effective monitoring tools. Using a combination of descriptive and experimental research methodologies, the study reviewed existing literature, gathered qualitative insights through student interviews, and conducted a thorough evaluation of a proposed smartphone-based proctoring system. The findings underscore the urgent need for real-time, technology-driven solutions to ensure fairness, reliability, and consistency in remote testing environments. The proposed system shows strong potential in mitigating these issues through the integration of advanced features such as facial recognition, voice activity monitoring, screen behavior tracking, and object detection. Together, these capabilities enhance the integrity of online examinations by enabling more accurate assessments of student performance and reinforcing the credibility of academic outcomes. Looking ahead, future research will focus on refining the system's technical performance, increasing its adaptability across various educational contexts, and deepening its integration with institutional learning management systems. Moreover, system development will extend beyond mobile access to the university platform by introducing monitoring capabilities that activate when a student opens their computer. This advancement aims to deliver consistent and comprehensive supervision across devices, paving the way for a more secure, scalable, and seamless remote assessment infrastructure that meets the evolving demands of digital education.

9. REFERENCES

[1] Ramzan, M., Abid, A., Bilal, M., Aamir, K. M., Memon, S. A., & Chung, T.-S. (2024). Effectiveness of pre-trained CNN networks for detecting abnormal activities in online exams. *IEEE Access*, 12, Article 3359689. https://doi.org/10.1109/ACCESS.2024.3359689

[2] Kassem, A., Falcone, Y., & Lafourcade, P. (2015). Monitoring electronic exams. In B. Bonakdarpour & S. A. Smolka (Eds.), *Runtime verification: 6th International Conference, RV 2015, Vienna, Austria, September 22–25, 2015, Proceedings* (Lecture Notes in Computer Science, Vol. 9333, pp. 118–135). Springer. https://doi.org/10.1007/978-3-319-23820-3_8

[3] Al_airaji , R. M. ., Aljazaery, I. A., Alrikabi, H. T., & Alaidi, A. H. M. . (2022). Automated Cheating Detection based on Video Surveillance in the Examination Classes. *International Journal of Interactive Mobile Technologies (iJIM)*, 16(08), pp. 124–137. https://doi.org/10.3991/ijim.v16i08.30157

[4] Copelan, L. (2013). *School cheating scandal shakes up Atlanta*. USA TODAY. http://goo.gl/wGr40s

[5] Valizadeh, M. (2022). *Cheating in online learning programs: Learners' perceptions and solutions*. *Turkish Online Journal of Distance Education*, 23(1), Article 12.

[6] Ngonadi, I. V., & Orobor, A. I. (2020). *Face recognition service model for student identity verification using deep neural network and support vector machine (SVM)*. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 6(4), 11–20. https://doi.org/10.32628/CSEIT2063225

[7] Gahan, C. J. (2004). URU — Online identity verification. *BT Technology Journal,* 22(1), 43–51. https://doi.org/10.1023/B:BTTJ.0000015494.59501.52

[8] Karakaş, E., Öztozlu, İ., & Erol, V. (2017). Two-factor authentication and its adaptation to online education systems. *Preprints*. https://doi.org/10.20944/preprints201706.0036.v1

[9] González Arrieta, A., López Sánchez, D., Sánchez Lázaro, Á. L., Pérez Lancho, M. B., García-Bermejo-Giner, J. R., Hernández Simón, J. A., & Vega Cruz, P. I.(2021).Two-step verification as a safety measure for learners and teachers: an attempt to implement it in a real environment,30129. https://ceur-ws.org/Vol-3129/paper108.pdf

[10] da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security, 92*, Article 101713. https://doi.org/10.1016/j.cose.2020.101713

[11] Alrikabi, H. T., & Tuama Hazim, H. (2021). Enhanced Data Security of Communication System Using Combined Encryption and Steganography. *International Journal of Interactive Mobile Technologies (iJIM),* 15(16), pp. 144–157. https://doi.org/10.3991/ijim.v15i16.24557

[12] Al-airaji, R. M., Aljazaery, I., & Alrikabi, H. T. S. (2022). Abnormal behavior detection of students in the examination hall from surveillance videos. *In Advanced computational paradigms and hybrid intelligent computing* (pp. 113–125). Springer. https://doi.org/10.1007/978-981-16-4369-9_12

[13] Appelbaum, D. A., Showalter, D. S., Sun, T., & Vasarhelyi, M. A. (2020). A framework for auditor data literacy*: A normative position. Accounting Horizons*, 35(2), 27–45. https://doi.org/10.2308/HORIZONS-19-127

[14] Shkodzinsky, O., & Kłos-Witkowska, A. (2023, June). Analysis of approaches to identity

verification during knowledge assessment in e-learning systems. *In Proceedings of the 1st International Workshop on Computer Information Technologies in Industry 4.0 (CITI 2023),* Ternopil, Ukraine, June 14–16, 2023.

[15] Barker, T., & Lee, S. (2007). *The verification of identity in online assessment: A comparison of methods*. Retrieved from https://www.researchgate.net/publication/48352512

[16] Kumar, T. S., & Narmatha, G. (2016). Video analysis for malpractice detection in classroom examination. *In Proceedings of the International Conference on Soft Computing Systems (Advances in Intelligent Systems and Computing*, pp. 135–146). Springer. https://doi.org/10.1007/978-81-322-2671-0_13

[17] Aubin, V., & Mora, M. (2017). A new descriptor for person identity verification based on handwritten strokes off-line analysis. *Expert Systems with Applications*, 89, 241–253. https://doi.org/10.1016/j.eswa.2017.07.053

[18] Karakaş, E., Öztozlu, İ., & Erol, V. (2017). Two-factor authentication and its adaptation to online education systems. *Preprints*. https://doi.org/10.20944/preprints201706.0036.v1

[19] Bawarith, R., Basuhail, A., Fattouh, A., & Gamalel-Din, S. (2017). E-exam cheating detection system. *International Journal of Advanced Computer Science and Applications (IJACSA),* 8(4), 176–181. https://doi.org/10.14569/IJACSA.2017.080425

[20] Ramzan, S., Sanjay, K. P., Al Tajiba, Shoeb, S., & D'Souza, K. J. (2019). Intelligent examination staff allotment system. *In Proceedings of RTESIT 2019. International Journal of Engineering Research & Technology (IJERT)*, 7(8). https://doi.org/10.17577/IJERTCONV7IS08089

[21] Sinha, P., Dileshwari, & Yadav, A. (2020). Remote proctored theory and objective online examination. *International Journal of Advanced Networking and Applications*, *11*(6), 4494–4500.

[22] Escobar-Grisales, D., Vásquez-Correa, J. C., Vargas-Bonilla, J. F., & Orozco-Arroyave, J. R. (2020). Identity verification in virtual education using biometric analysis based on keystroke dynamics. *TecnoLógicas*, 23(47), 197–211. https://doi.org/10.21500/22565337.4315

[23] Qi, G., Hu, G., Wang, X., Mazur, N., Zhu, Z., & Haner, M. (2021). EXAM: A framework of learning extreme and moderate embeddings for person re-ID. *J. Imaging, 7*(1), 6. https://doi.org/10.3390/jimaging7010006

[24] Sahane, S. N., Khapare, M. V., Dughad, S. S., Ambekar, A. R., & Sonawane, V. A. (2024). Theory exam conductor and management system. *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT),* 4(3), 2581-9429. https://doi.org/10.48175/IJARSCT-15519

[25] Vijaypriya, V., Dhanesh, P. M., Giridhar, V., & Harish, B. L. (2024). A multifaceted approach to real-time online proctoring with gaze tracking, facial aspect ratio analysis, and object detection. *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT),* 4(4). https://doi.org/10.48175/IJARSCT-15937

[26] Narayana, K. L., Dinesh, G., Kumar, K. K., Adithya, P. P., Sai, M. H. V. S., & Reddy, V. C. M. (2025). Online exam proctoring. *International Journal of Innovative Science and Research Technology, 10*(4). https://doi.org/10.38124/ijisrt/25apr798