# Securing exams using mechatronics

*By*

*A. E. E. ElAlfi*
*Department of Computer Science*
*Faculty of Specific Education*
*Mansoura, Egypt*

*A. F. Al-Jamal*
*Department of Computer Science*
*Faculty of Specific Education*
*Mansoura, Egypt*

*M. M. Saad*
*Department of Computer Science*
*Faculty of Specific Education*
*Mansoura, Egypt*

**Research Journal Specific Education**
**Faculty of Specific Education**
**Mansoura University**

**ISSUE NO. 83 MAY , 2024**

# Securing exams using mechatronics

A. E. E. ElAlfi * A. F. Al-Jamal* M. M. Saad*

## Abstract

This paper presents methods to prevent cheating and leaking using internet of things. Related technologies are used to minimize or prevent cheating and leaking through some proposed solutions. Before the exam, RFID is integrated into the student's card to identify the student’s information record. During the exam, a sound sensor is used to monitor the sounds inside the exam hall. The last stage, which is after the exam, a motion sensor was used to secure the location of  exam papers to avoid any unauthorized person infiltrating the place by sending an alarm sound or a light warning.  The solutions include an integrated Arduino Mega 2560 board, an MFRC522 RFID reader, in addition to an ESP8266 Board. The modern software tools supported are the Arduino Integrated Development Environment (IDE), XAMPP, Apache HTTP Server, MySQL and PHP My Admin.

**Keywords**: Exam leakage, Cheating, Speech detect,  Smart card readers, RFID

## 1. Introduction

With the rapid advancement of the internet and technology over the past ten years, relying solely on traditional methods to detect cheating may no longer be sufficient to completely prevent dishonest behavior during exams. Exams serve as a fundamental method for assessing students' knowledge and are generally divided into three categories: traditional exams, online exams, and distance exams (D-exams). Traditional exams take place in a classroom, where students answer a fixed set of questions within a given time limit. Online exams, also called e-examinations, are conducted via the internet, with questions randomly assigned from a pool and a specific time frame for completion. Despite being online, students must still be physically present in an examination room to take the test.  [1].

* Department of Computer Science Faculty of Specific Education Mansoura, Egypt

D-exams are designed for students who are not physically present in a traditional classroom setting. These exams generate questions randomly for each student and must be completed within a set time limit. In addition to reducing the time spent on grading, they also help conserve paper and printing materials, promoting environmental sustainability. However, they present a major challenge for educators—preventing academic dishonesty. To address this, many e-learning institutions require students to take exams at specific locations within the institution under supervision to verify their identity. This requirement, however, conflicts with the fundamental goal of e-learning, which is to eliminate time and location constraints, as students must still be physically present to take the exam. [2].

This paper examines various techniques used for cheating in exams and addresses this issue through strategies focused on either detection or prevention.

## *2. Stages of examination processes:*

Cheating is acting dishonestly or unfairly to gain an advantage. Cheating is unethical and most students know that it is fundamentally wrong. There are many types of cheating (academic cheating, cheating in personal relationships, athletic cheating, cheating in games and gambling), but here we will focus on academic cheating [3].

Exam cheating is a common issue worldwide, regardless of advancements in detection methods. Over the past decade, numerous studies have explored students' cheating behaviors and examined strategies that universities can use to address this challenge [4].

There are many methods to prevent cheating and leaking.

### i. Before exam:

Student's identification (SID) before entering classroom exam ensuring proper student's identification is essential to maintain exam integrity. Here are some common methods to achieve (SID):

1. **Student ID**: Require students to present their official student identification cards or university-issued IDs at the entrance.
2. **Biometric Verification**: Use biometric authentication methods such as fingerprint or facial recognition to verify students' identities. This can be done through specialized devices or software [5].

3. **Smart Cards Radio Frequency Identification (RFID)**: Implement smart card systems where students tap or scan their cards to gain access to the exam room. These cards can contain embedded information for identity verification [6].
4. **QR Codes**: Generate unique QR codes for each student and scan them at the entrance to verify their identity against a database [7].

It is crucial to strike a balance between security and efficiency. The chosen method should be practical for the number of students and resources available. Additionally, consider privacy concerns and ensure that any data collected for identification purposes were handled in compliance with relevant privacy regulations.

**ii. During exam:**

Student observation during exam time is important to maintain exam integrity and prevent cheating. Here are some key considerations for effective student observation:

1. **Development Proctors:** Ensure that exam proctors or invigilators are well-trained to observe students without causing discomfort or disruption [10].
2. **Seating Arrangements:** Arrange student seating to minimize the opportunity for cheating, such as sitting them apart from one another or using randomized seating[11].
3. **Clear Guidelines:** Communicate clear exam rules and guidelines to students before the exam, including expectations regarding behavior and what constitutes cheating.
4. **Constant Vigilance:** Proctors should maintain constant vigilance, moving around the exam room and monitoring students for suspicious behavior.

**iii. After exam:**

Controlling and ensuring the assurance of exam results is crucial for maintaining the integrity of the assessment process. Here are steps and strategies to achieve this:

1. **Secure Storage of Exam Papers:** Ensure that physical exam papers are securely stored before and after the exam to prevent tampering or unauthorized access.
2. **Digitization of Exams:** Consider using digital exams and assessment platforms to reduce the risk of paper-based exam mishandling and to maintain a digital record [12].
3. **Access Control:** Restrict access to exam papers, answer keys, and assessment systems to authorized personnel only. Implement strong authentication and authorization mechanisms [13].

4.**Monitoring and Auditing:** Regularly monitor and audit the exam process, including paper handling and digital systems, to detect any irregularities or security breaches [14].

5.**Data Backup:** Regularly back up digital exam data to prevent loss due to technical issues or data corruption [15].

## 3.Experimental work:

**Part illustrates experimental work for the proposed system**

### 3.1 Before Exam:

**Radio Frequency Identification (RFID)**

**Table 1: shows the hardware components involved in the experiment:**

| S.N | COMPONENTS NAME | DESCRIPTION | QUANTITY |
|---|---|---|---|
| 1 | NodeMcu | ESP8266 12E Board | 1 |
| 2 | RFID Module | RFID-RC522 Module | 1 |
| 3 | Jumper Wires | Male to Male Jumper Wires | 4 |
| 4 | Breadboard | Solderless Breadboard Mini | 1 |

**the software components**:

- ✓ Arduino IDE
- ✓ XAMPP server
- ✓ PHP Source Code
- ✓ RFID-RC522 Library
- ✓ NodeMcu ESP8266 Library and Board Manager

The design and development of this recognition and registration system require both hardware and software components. On the hardware side, the system consists of four key elements: the embedded board (Arduino ESP8266 12E), an RFID reader (MFRC522), a network adapter, and a breadboard. The MFRC522 RFID reader operates at a frequency of 13.56 MHz and complies with the ISO/IEC 14443 communication standard, which plays a vital role in selecting the appropriate type of RFID tag for the system. To power the Arduino board, the AC/DC power adapter 0910 is used.

On the software side, the Arduino Integrated Development Environment (IDE) is utilized for programming the ESP8266 12E Board. This cross-platform application supports C and C++ programming languages, enabling the writing and uploading of code to the board. Additionally, the system uses open-source cross-platform web server tools, including XAMPP, Apache HTTP Server, MySQL, and PhpMyAdmin, to develop and manage the web server.

The web server is responsible for storing important data related to student exam entries and other relevant details needed for the check-in verification process. This verification process involves the web server confirming the authenticity of an attendance request received from the interfacing device. The web server architecture is organized into two main parts: the backend and the frontend. The backend handles the database management and server-side operations.

The database is used to store essential information, while the server-side software manages backend tasks initiated by requests from the frontend. The frontend framework is a web-based interface that allows users to interact with the system, built using client-side programming tools. The role of the interfacing device is to read student ID cards and send verification requests to the web server.

This interfacing device is made up of three peripherals connected to an embedded board, which acts as the controller, managing the operations of these peripherals. The RFID tag contains the student’s ID details needed for the check-in process. The main components used in the interfacing device include the ESP8266 12E Board, an RFID reader, and a network adapter. The RFID reader is responsible for scanning student ID cards, while the network adapter provides the necessary network connection.

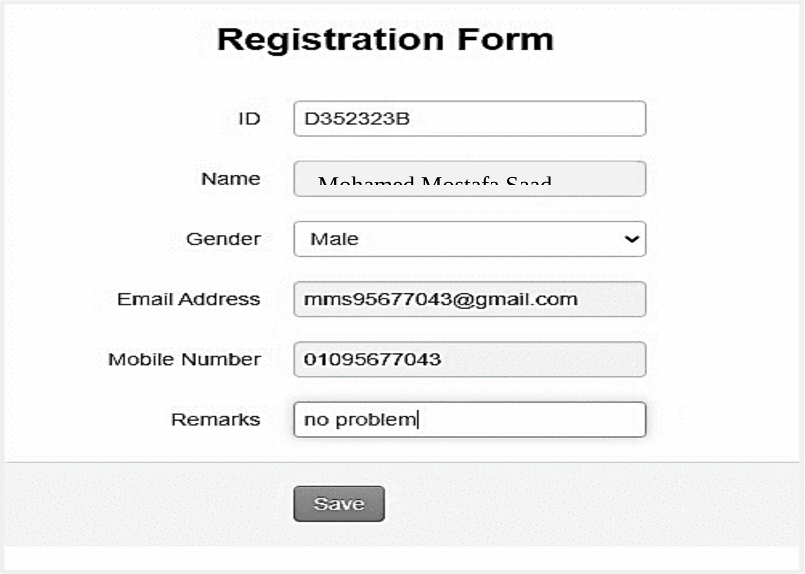
Unlike typical devices, the interfacing device does not need a graphical user interface or a web browser. It only requires an Ethernet shield to send HTTP requests to the web server and receive the corresponding responses. Acting as a bridge, the networking device links the interfacing device and users to the web server. The router connects the web server, interfacing device, and users to the network, ensuring that data packets are correctly routed to their destinations.

After the verification process, the web server sends a response to the interfacing device regarding the verification of the student's identity. If the card is valid, the student is allowed to enter the exam. If the card is invalid, the student is not permitted to enter the exam. If there is an issue with the card, the student should go to the administration to resolve the problem.

Connecting an RFID reader with Arduino and sending data to a PHP server over the internet using HTTP:

```
#include <ESP8266WiFi.h>
#include <ESP8266HTTPClient.h>
#include <SPI.h>
#include <MFRC522.h>
#define SS_PIN D4
#define RST_PIN D3
MFRC522 rfid(SS_PIN, RST_PIN);
const char* ssid = "your-SSID";
const char* password = "your-PASSWORD";
String serverPath = "http://your-server.com/rfid.php";
void setup() {
  Serial.begin(115200);
  SPI.begin();
  rfid.PCD_Init();
  WiFi.begin(ssid, password);
  while (WiFi.status() != WL_CONNECTED) {
    delay(1000);
    Serial.println("Connecting to WiFi...");
  }
  Serial.println("Connected to WiFi");
}
void loop() {
  if ( ! rfid.PICC_IsNewCardPresent() || ! rfid.PICC_ReadCardSerial() ) {
    return;
  }
   String uid = "";
  for (byte i = 0; i < rfid.uid.size; i++) {
    uid += String(rfid.uid.uidByte[i], HEX);
  }
  uid.toUpperCase();
  Serial.print("Card UID: ");
  Serial.println(uid);
  if (WiFi.status() == WL_CONNECTED) {
    HTTPClient http;
        String fullServerPath = serverPath + "?uid=" + uid;
    http.begin(fullServerPath);
    int httpResponseCode = http.GET();
    if (httpResponseCode > 0) {
         String response = http.getString();
      Serial.println(httpResponseCode);
      Serial.println(response);
    } else {
      Serial.print("Error on sending GET: ");
      Serial.println(httpResponseCode);
    }
    http.end();
  }
  delay(5000);
}
```

In this step, we place the card on the device. The device reads the number stored inside the card, which then appears in the first field of the registration form and on the Arduino screen. Next, we complete the registration by entering the remaining data and then save it, as shown in **Figure 1**.



Registration Form

| | |
|---|---|
| ID | D352323B |
| Name | Mohamed Mostafa Saad |
| Gender | Male |
| Email Address | mms95677043@gmail.com |
| Mobile Number | 01095677043 |
| Remarks | no problem |

**Figure 1**: Registration form

Thus, the experiment results are as shown in the following **Table 2**.

**Table 2**: Result used card and similar card

| S.N | Case | Response |
|---|---|---|
| 1 | Student Register | Enter exam |
| 2 | Student Not Register | Deny exam |
| 3 | Student with similar card | Deny exam |

……………………………………………………………………………………..

### 3.2 During exam:

**Speech sensor**

**Detect speech component Hardware:**

- Arduino
- A Sound Sensor
- LED
- 220 ohm Resistors

- Mini Breadboard
- Wires

The purpose of using this technique is to determine whether there is any disturbance in the sound in the evaluation board and whether the pitch of the sound increases or not as shown in **Figure 2**.

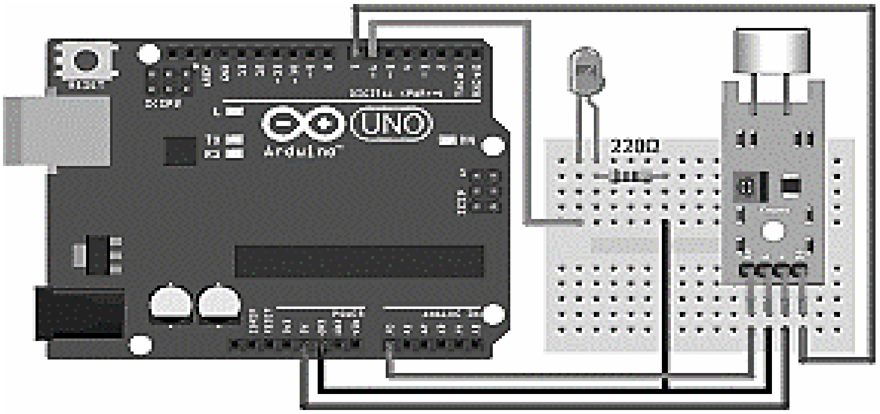


**Figure 2**: Speech detection sensor connection

**Code**:

```
int led = 13;
int threshold = 28;
int volume;
void setup() {
  Serial.begin(9600);
  pinMode(led, OUTPUT);
}
void loop() {
  volume = analogRead(A0);
  Serial.println(volume);
  delay(100);
  if (volume >= threshold) {
    digitalWrite(led, HIGH);
  } else {
    digitalWrite(led, LOW);
  }


}
```

### 3.3 After exam:

**Motion sensor**

1 **- Design**:

The development of this motion sensor goes through multiple manufacturing stages. It starts with gathering and preparing the necessary materials and tools, including setting up the light lamp and power source. The next step is assembling the electronic circuit for the motion sensor system. This systematic approach guarantees that all components are properly prepared and assembled to create an effective motion sensor system..

2 - **component Hardware** as shown as **Figure 3**:

- 1 × Breadboard
- 1 × Arduino Uno R3
- 1 × PIR Sensor (MQ3)
- 1 × LED lamp
- 1 × Buzzer

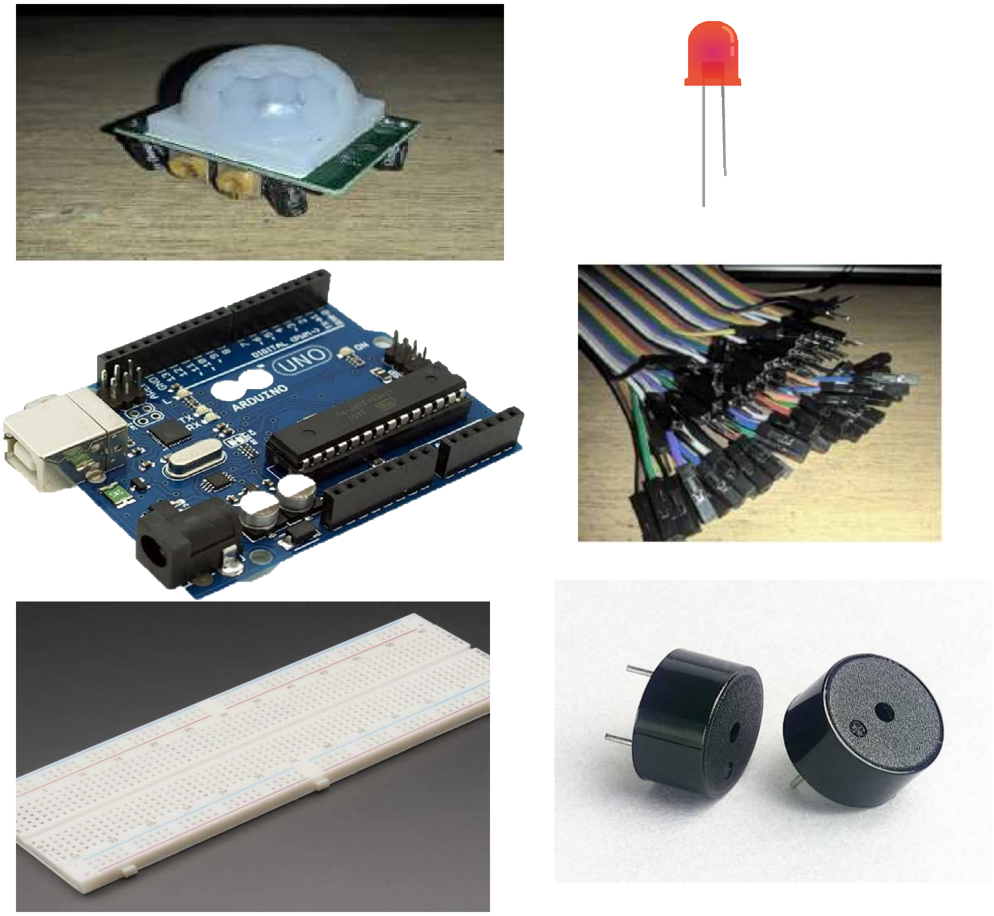
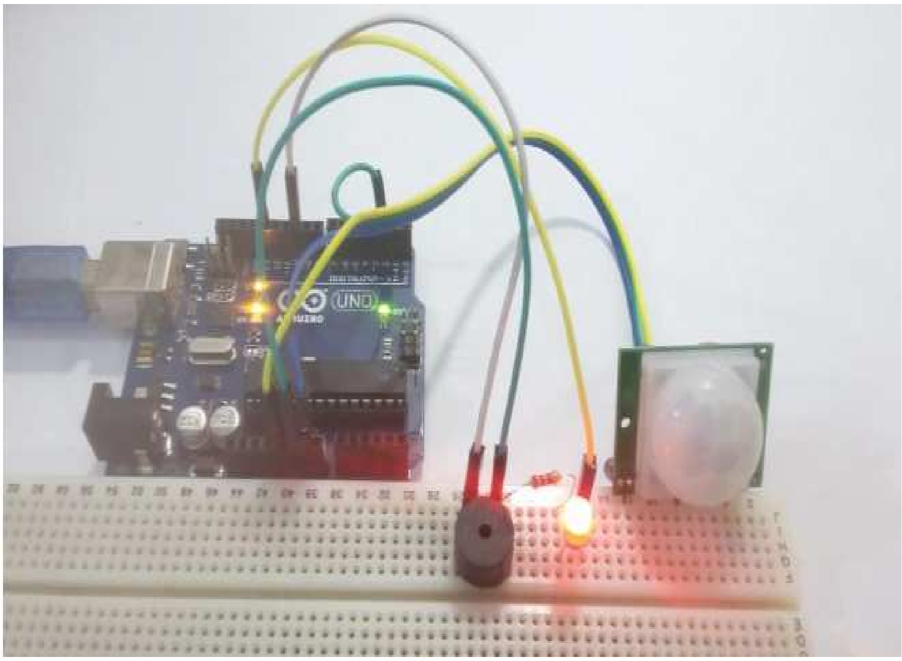


**Figure 3:** Tools and Material

**Code:**

```
PIR Sensor code for Arduino Uno
const int PIR_SENSOR_OUTPUT_PIN = 4;
int warm_up;
void setup() {
  pinMode(PIR_SENSOR_OUTPUT_PIN, INPUT);
Serial.begin(9600);
delay(20000);
}
void loop() {
  int sensor_output;
  sensor_output = digitalRead(PIR_SENSOR_OUTPUT_PIN);
  if( sensor_output == LOW )
  {if( warm_up == 1 )
     {Serial.print("Warming Up\n\n");
      warm_up = 0;
      delay(2000);
    }
    Serial.print("No object in sight\n\n");
    delay(1000);
  }
  else
  {
    Serial.print("Object detected\n\n");
    warm_up = 1;
    delay(1000);
  }
}
```

**Implementation:** The sensor measures changes in infrared radiation emitted by objects, in this case, humans. It does not measure the total amount of infrared rays from a person, but rather the changes in these rays, allowing it to detect movement. When a person moves in front of the sensor, the amount of infrared radiation received by the sensor changes, indicating the presence of someone. Upon detecting movement, the sensor sends a signal to the Arduino, which then activates the buzzer and lights the LED to provide an alert, as shown in Figure 4



.

The system's motion detection capability is tested at distances ranging from 3 to 8 meters. When someone moves in front of the PIR sensor, the lights turn on, showing that the sensor can reliably detect motion at distances of up to 8 meters.

## 4. Conclusion:

Cheating and leaking have become widespread, with students increasingly depending on them rather than focusing on their studies. In our study, we have identified a potential method to reduce reliance on cheating and reinforce values in students by emphasizing learning, through the use of connectivity devices and mobile testing tools, in addition to audio programming.

## Reference:

[1]. Razan Bawarith, Dr. Abdullah Basuhail, Dr. Anas Fattouh and Prof. Dr. Shehab Gamalel-Din. *E-"exam Cheating Detection System"*, (IJACSA) International Journal of Advanced Computer Science and Applications ,Vol. 8, No. 4, 2017.

[2] Razan Bawarith, Dr. Abdullah Basuhail, Dr. Anas Fattouh and Prof. Dr. Shehab Gamalel-Din. " E-exam Cheating Detection System ",International Journal of Advanced Computer Science and Applications, Vol. 8, No. 4, 2017.

[3]. Hao, Jiangang. *"The Detection of Cheating on E-Exams in Higher Education—The Performance of Several Old and Some New Indicators". October 2020 | Volume 11 | Article 568825*.

[4]. Ajasa, A.A. and al, and et. "*Design and Development of a Mobile Phone Signal Detector",* The Pacific Journal of Science and Technology, Volume 15. Number 2. November 2014 (Fall).

[5]. Bain, Lisa Z." *How Students Use Technology to Cheat and What Faculty Can Do About It", Information Systems Education Journal,V13 N5 Pages 92-99,* September 2015.

[6]. AlexandruTopirceanu, AlexandraDuma,MihaiUdrescu. *"Uncovering the fingerprint of online social networks using a network motif based approach",*2015 Elsevier B.V, *Volume 73, Part B, 1 January 2016, Pages 167-175.*

[7]. Krishnan, V. *Application of RFID technology in Library: A view,* International Journal of Library and Information Studies, Vol.4 (2) Apr-Jun, 2014, ISSN: 2231-4911.

[8]. Topîrceanu, Alexandru. *Breaking up friendships in exams: A case study for minimizing student cheating in higher education using social network analysis.* 2017 : s.n.

[9]. Neil Selwyn, Chris O'Neill. *A necessary evil? The rise of online exam proctoring in Australian universities, Media International Australia,Volume 186, Issue 1, February 2023, Pages 149-164*

[12]. Balázs Keresztury *, László Cser. *New cheating methods in the electronic teaching era,* ,Procedia - Social and Behavioral Sciences 93 ( 2013 ) 1516 – 1520.

[13]. *MacKevett, Douglas and Gutmann, Martin. High-Stakes Online Exams: Faculty Perceptions on Forced Digitization of Assessment During Corona at a Swiss Business School.,* International Journal of Emerging Technologies in Learning iJET | Vol. 18 No. 13 (2023).

[14]. *Dun Li, Dezhi Han. A blockchain-based secure storage and access control scheme for supply chain finance.,* Sensors 2023, 23, 7036. https://doi.org/10.3390/s23167036.

[15]. Esraa Esam Alharasis, Manal Alidarous. Corporates' monitoring costs of fair value disclosures in pre- versus post-IFRS7 era: Jordanian financial business evidence, COGENT BUSINESS & MANAGEMENT2023, VOL. 10, NO. 2.

## الملخص العربي

تقدم هذه الورقة طرقًا لمنع الغش والتسريب باستخدام إنترنت الأشياء. يتم استخدام التقنيات ذات الصلة لتقليل أو منع الغش والتسريب من خلال بعض الحلول المقترحة. قبل الامتحان، يتم دمج RFID في بطاقة الطالب لتحديد سجل معلومات الطالب. أثناء الامتحان، يتم استخدام مستشعر الصوت لمراقبة الأصوات داخل قاعة الامتحان. المرحلة الأخيرة، وهي بعد الامتحان، تم استخدام مستشعر الحركة لتأمين مكان أوراق الامتحان لتجنب تسلل أي شخص غير مصرح له إلى المكان عن طريق إرسال صوت إنذار أو تحذير ضوئي. تتضمن الحلول لوحة Arduino Mega 2560 مدمجة وقارئ RFID MFRC522 بالإضافة إلى لوحة ESP8266. أدوات البرمجيات الحديثة المدعومة هي بيئة التطوير المتكاملة (IDE Arduino) و XAMPP و Apache HTTP Server و MySQL و PHP MyAdmin.