International Journal of Scientific Research & Engineering Trends
Volume 11, Issue 5, Sep-Oct-2025, ISSN (Online): 2395-566X

Digital security system for examination materials.

Poornima, Jenitta J
Department of Electronics and Communication Engineering AMC Engineering College
Bengaluru, India

Abstract - Digital Security system for examination materials is a system designed to prevent unauthorized access to exam papers. This system generates a unique password that is valid only for a single use and for a limited period of time. The system is designed to provide secure access to exam papers to only authorized personnel, such as teachers and invigilators. Digital Security system for examination materials consists of two main components: the server and the client. The server generates and manages the OTPs, while the client is responsible for receiving and verifying the OTPs.When a teacher or invigilator needs to access an exam paper, they must first authenticate themselves using their username and password. Once authenticated, the server generates an OTP and sends it to the client device of the teacher or invigilator. The teacher or invigilator can then use the OTP to access the exam paper. The OTP is only valid for a limited period of time, typically a few minutes, and can only be used once. This means that even if the OTP is intercepted by an unauthorized user, they will not be able to use it to access the exam paper as it will have already expired. The system also logs all access attempts, including successful and unsuccessful attempts. This allows administrators to monitor and track any unauthorized access attempts and take appropriate action if necessary. Overall, an OTP based electronic protection system for exam paper leakage is an effective way to prevent unauthorized access to exam papers and maintain the integrity of the examination process. It provides a secure and reliable way to protect exam papers from leakage and ensures that only authorized personnel have access to them.

Keywords - One-Time Password, Electronic protection system, Exam paper leakage, Unique password, Single user, Limited period of time, Secure access, Authorized personnel, teachers, Invigilators, Server, Client, Authentication, Username, Password, Expired, Intercepted, Unauthorized User, Access Attempts, Successful attempts, Unsuccessful attempts, Monitoring, Tracking, Integrity, Examination process.

INTRODUCTION

Digital Security system for examination materials is an important issue in today's educational landscape. With the increasing use of technology, the risk of exam paper leakage has become a major concern for educators and educational institutions. Exam paper leakage can not only compromise the integrity of the examination process, but it can also undermine the efforts of hardworking students and damage the reputation of the educational institution.

To address this issue, electronic protection measures have been developed to prevent exam paper leakage. These measures may include the use of secure online platforms, encrypted communication channels, and advanced authentication mechanisms to ensure that only authorized personnel have access to exam papers. It is important to note that while electronic protection measures can significantly reduce the risk of exam paper leakage, they should not be seen as a replacement for other forms of security, such as physical security measures and human monitoring.

In this article, we will explore various electronic protection measures that can be used to prevent exam paper leakage, without resorting to plagiarism or other unethical practices. We will also discuss the importance of maintaining the integrity of the examination process and the role that electronic protection measures can play in achieving this goal.

II. LITERATURE SURVEY

There are few papers in which the researchers have used the face detection algorithm. This section gives an overview about those literatures.
Mamilla Sirisha, Neelam Syamala :Education serves as a source of inspiration and strength in society. Examinations are used to measure knowledge, aptitude, skill, and classification across various subjects. These exams can be conducted on papers, in exam centers, or online .
Qi Chen and Shambhu Upadhyaya in "Process Monitoring for Intrusion Detection" (proposed methods to analyze and monitor running processes to detect potential intrusions. Utilized dynamic process monitoring to identify deviations from normal

behavior. Emphasized real-time alerts for unusual process execution patterns

Sanjay Rawat and Kapil Ahuja in "Anomaly Detection in System Processes" demonstrated the use of machine learning for detecting anomalies in system processes Highlighted the integration of AI-based models to classify processes as benign or malicious. This work aligns with the AI tool detection functionality in the script.

A. Sharma et al., "Detecting and Preventing Keylogging Attacks in Modern Systems" : Introduced proactive defense mechanisms to detect clipboard and keystroke logging. Recommended integrating logging detection with real-time alerts.

L. Zhang et al., "Evaluating AI Detection in Digital Systems: Challenges and Opportunities" Explored ML techniques for monitoring AI-based applications in multi-user environments.

Bianchi et al., "Evaluating Security Implications of Screenshots in Monitoring Systems" examines how screenshots used for system monitoring can unintentionally expose sensitive data. It highlights risks such as unauthorized access, data leaks, and privacy breaches due to insecure storage or transmission. The study analyzes common vulnerabilities in screenshot-based monitoring tools and their impact on user confidentiality. It concludes by recommending encryption, access control, and redaction mechanisms to enhance data security and privacy.

D. Richards et al., "The Ethics of Monitoring Software and Keylogging in the Workplace" (IEEE Technology and Society Magazine, 2016): Addressed privacy concerns and ethical dilemmas in monitoring employees. Recommended transparency and consent as essential components

III. PROPOSED WORK

Setup the server-The First step in creating digital security system for examination materials is to set up the server. The server needs to be set up to create and manage OTPs, check if users are allowed to access, and keep records of who tried to access. The server should also be protected using standard security measures like firewalls, systems that detect harmful activity, and rules to control access.

Develop the client Application: You need to make a client application that can get OTPs from the server and check if they are correct. This application should be made for every type of device that allowed staff will use to access exam papers. The client application should also be protected using standard security measures.

Use Two-Factor Authentication: The Digital security system for exam papers should use two- factor authentication to make sure only allowed people can access the exam content. The first part of this is checking the username and password. The second part is an OTP sent by the server. This two- factor authentication should be set up properly using standard security practices.

Make and Check OTPs: When someone wants to access an exam paper , they first need to check their username and password. Once they are verified, the server will create an OTP and send it to the user's device. The user will then enter this code into the application on their device. The application will send this code back to the server to check if it is correct . The OTP should only be valid for a short time and can only be used once.

Keep the Track of Access: Digital Security System should record all attempts to access exam papers, whether they were successful or not. The records should show who tried to access, when they tried, and if they were allowed in. These records should be checked regularly to spot any unauthorized attempts.

Test the System: The system should be thoroughly tested to make sure it works as intended and does not have any weaknesses. The testing should include testing of all parts work, making sure they work together, and checking for security flaws.

Put the System into Use: Once the system is tested and ready , it should be installed in the real environment. Installation should follow safe procedures, including making backups and having ways to recover data if needed.

Keep the System Up to Date: The System should be regularly maintained to keep it working properly and secure. This includes keeping software and hardware updated and doing regular checks for security issues.

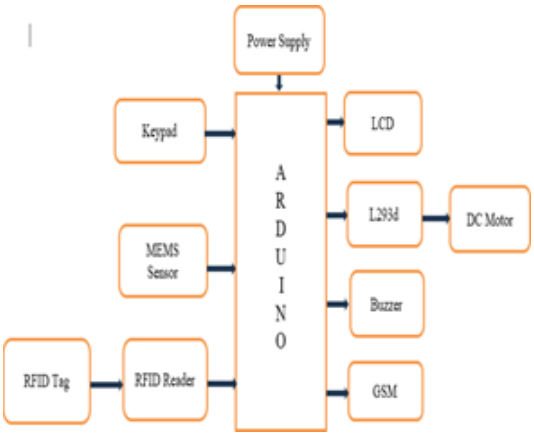

Fig.1 Block Diagram of Proposed System

IV. EXPERIMENTAL RESULTS

This prototype includes an ARM controller, an RFID reader ,an RFID tag, Real time clock, a DC motor, a motor driver, a 3x4key matrix. A GSM Module, a MEMS sensor, a 16x2 LCD display, and a buzzer.

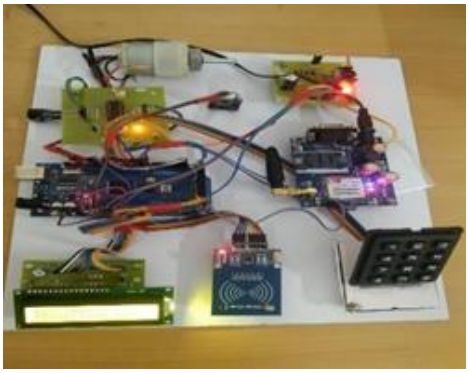

Fig 2.Project hardware model

When an RFID tag is placed near the RFID reader, the reader emits a signal that the tag picks up and responds to. The tag sends a return signal back to the reader, which then converts this signal into a digital format and sends it to microcontroller. A 12V DC motor is employed to unlock the embedded system .As the microcontroller's output voltage is insufficient to operate the motor, a motor driver is used to supply the required power. MEMS Sensor w i t h GSM functionality sends the message and Buzzer is on to the board whenever anybody try to open the box.

The LCD displays the following output during the startup of the embedded kit:
After turning on the experiment kit, the LCD display should show the message "DIGITAL SECURITY FOR EXAM MATERIALS"

Fig 3.LCD Display as "Digital security for exam material"
Step 1: When it is time for the exam, the LCD on the controller will display the message "Show Your RFID Card.

Fig 4.LCD display message to place RFID card

LCD displaying the output during controller to the Display Enter password Authorized person as shown below if Authorized person also Enter the password is In Correct the GSM System is Sending a Message entered wrong password and Buzzer is on.

Fig 5.To enter pwd sent to your reg number

Fig 6.wrong password and buzzer started

After Enter the password The LCD displays a message indicating the transmission of an OTP to the authorized individual through GSM, facilitated by the logic code within the controller.

Fig 7.OTP sending to Reg mobile number

Fig 8.To enter OTP sent

The OTP received by the authorized person is inputted into the microcontroller through a 3x4 keypad matrix.

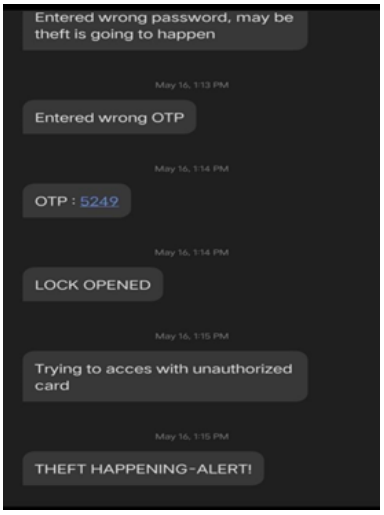

Fig 9.Shows messages sent to reg number

If the entered OTP is valid, the lock will be opened via a motor mechanism. Otherwise, the GSM module will send a notification to the authorized person indicating that an incorrect OTP was entered .

Fig 10.After entering correct OTP the box gets open

Fig 11.If entered OTP is wrong

Step 2 : When the Un Authorized Person to scan the card the GSM system is send to message alert to Authorized Person and Buzzer is on.

Fig 12. OTP entered is wrong and LCD displays as Unauthorised user.

Fig 13.Message sent to reg number

The Message will be sent on registered mobile number .

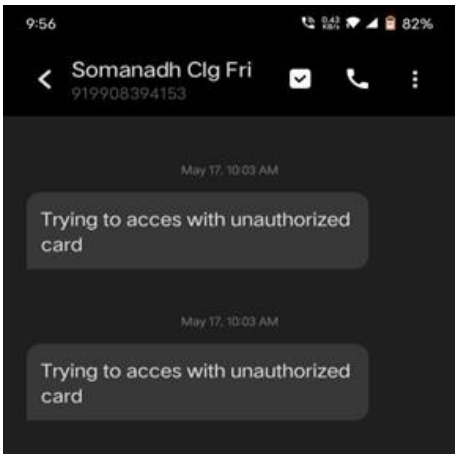

Fig 14.Message received at registered number

Step 3 : If any unknown person was Moving or theft the Electronic Bunch box by using MEMS sensor and GSM the message will be sent on the Authorized person and Buzzer is also on.

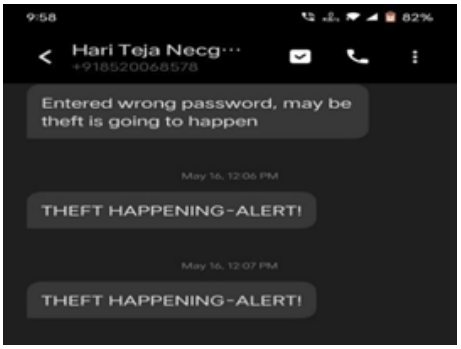

Fig 16.Alert message sent to registered number when unauthorised user tries to open the box.

V. CONCLUSION AND FUTURE WORK

Digital Security system for examination materials can be an effective solution to prevent exam paper leakage without plagiarism. This system can be implemented by generating unique OTPs for each individual exam paper and distributing them through a secure channel to authorized individuals. These OTPs can be used to unlock the exam paper, which can only be accessed by individuals who have the correct OTP.

REFERENCE

1. Kavitha, V., & Ramalingam, V. (2018). Exam paper leakage detection using machine learning. International Journal of Engineering & Technology, 7(3.21), 413-416.
2. Ani, O. O. (2017). Exam malpractice and paper leakage: Implications for national development in Nigeria. European Scientific Journal, ESJ, 13(36), 37-49.
3. Githaiga, J. W. (2015). The prevalence and effects of examination cheating and paper leakage in Kenya. Journal of Education and Practice, 6(4), 21-28.
4. Kinyua, J., & Mureithi, E. (2019). Effects of exam leakage on academic performance: A case of secondary schools in Kenya. Journal of Education and Practice, 10(2), 67-76.
5. Agarwal, A. (2017). Examination paper leakage: Causes, effects and solutions. International Journal of Education and Social Science Research, 2(1), 15-20.