International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 05 | May - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Electronic Protection for Exam Paper Leakage

M. Uma Rani[1], M.Deekshitha[2], G. Rishith Reddy[3]
[1]Senior Assistant Professor, Dept of Electronics and Communication Engineering, Geethanjali College of Engineering and Technology, Telangana, India
[2,3]Students , Dept of Electronics and Communication Engineering, Geethanjali College of Engineering and Technology, Telangana, India

---

Abstract:

The project aims to address the growing Concerns surrounding the security and confidentially of Exam papers within educational institutions. Exam Paper Leakage has become a major issue, often leading to unfair Advantages, comprised academics integrity, and significant Reputational damage to institution. Traditional methods of exam paper management, such as physical storage and manual distribution, have proven to be vulnerable to unauthorized access and breaches. The project describes electronic protection for exam paper leakage which is a highly security system. Question paper comes to the college from university in electronic sealed box which is an embedded system designed with raspberry pi pico. An RFID card will be given to the authorities and password will send to college before 10 minutes of exam. By swiping the card with appropriate Password, lock of electronic sealed box is open. If anyone Tries to open the electronic sealed box before and after RFID swipe duration, message will be send to university board through GSM which indicates exam paper is leaked.

Key Words: RFID, GSM, Raspberry pi pico

1.INTRODUCTION

In today's digital era, maintaining the confidentially and security of examination papers is a critical concern for educational institutions. Incidents of exam paper leaks have not only compromised academic integrity but have also eroded trust in the evaluation process. Traditional methods of paper distribution. Such as Manual handling or physical storage are highly Susceptible to unauthorized access, tampering.

To combat these vulnerabilities, this project process A smart, embedded system titled "Electronic Protection For Exam Paper Leakage." It integrates modern Technologies like RFID authentication, GSM communication, password-based access control, and Real-time alert mechanisms to ensure secure exam Paper delivery.

The core of the system is built on a Raspberry Pi Pico microcontroller. Exam papers are securely stored in an electronic sealed box that opens only When both a valid RFID card and a one time password (OTP) are authenticated just before the examination begins. If any unauthorized access is attempted outside the designated time window, the system triggers a GSM alert to notify the university or administrator instantly.

This solution not only automates and secures the question paper distribution process but also serves as a deterrent to potential breaches, ensuring enhanced transparency and accountability in academic institution .

2. LITERATURE REVIEW

The issue of examination paper leakage has become a serious concern for academic institutions, threatening the integrity of the education system and damaging institutional reputation. Over the past decade, numerous efforts have been made to develop technological solutions that ensure the confidentiality and secure handling of exam question papers. Traditional methods—such as manual transportation, physical safes, and time-based invigilation—have proven to be unreliable due to human errors, insider threats, and lack of real-time surveillance.

To address these gaps, researchers have turned to embedded systems and digital security technologies. In [1], the use of RFID-based authentication was proposed to control physical access in academic institutions. The study highlighted how RFID cards, assigned to authorized personnel, can prevent unauthorized access to sensitive areas and materials. Due to their cost-effectiveness and ease of integration, RFID systems are ideal for educational settings.

In another study [2], GSM-based alert mechanisms were implemented to notify authorities in real time during unauthorized access attempts. The GSM module, when integrated into an embedded control system, allows automatic messaging to a central authority if a breach is detected. This proactive alert system ensures rapid response and improves accountability.

Further advancements include the use of Raspberry Pi and microcontroller-based systems for document protection and digital sealing, as discussed in [3]. These systems offer automation, OTP/password protection, timestamp logging, and secure data storage, thereby improving both physical and digital security.

A notable development was presented in [4], where a hybrid locking mechanism combined password-protected access and electronic monitoring to prevent tampering during the transport and storage of examination papers. The approach effectively reduced human involvement and ensured that only authorized users could retrieve the exam papers at a scheduled time.

Although these individual technologies show promise, very few studies have combined them into a single, integrated system tailored specifically for exam

paper protection. This project aims to fill that void by developing a smart, embedded system using Raspberry Pi Pico, RFID verification, OTP/password protection, and GSM alerts. The solution offers a layered security model that detects, reports, and prevents unauthorized access, ensuring a tamper-proof and traceable process for examination paper management.

3. PROBLEM DEFINATION

The manual handling and distribution of examination papers often lack proper security mechanisms, making them vulnerable to authorized access and tampering. In many cases, there are no alert systems in place to inform authorities in real time about breaches, which leads to paper leaks and compromises the integrity of the examination process.

To overcome these challenges, this project introduces a dual-layer electronic protection system for securing question papers. The first layer of security involves an RFID-based access control, where each college is issued unique RFID card by the university. This restricts access only to authorized personnel.

The second layer utilizes a keypad interface for date, time, and password verification, adding another level of protection. Furthermore, a GSM module is integrated to send immediate alerts to university officials if any unauthorized access or tampering is detected. This layered approach ensures real-time monitoring and strengthens examination paper security.

4. SYSTEM IMPLEMENTATION AND WORKING

The block diagram consists of power supply section,
16X2 LCD Display, 4 X 3 keypad, GSM, Raspberry pi Pico, Servo motor, Buzzer, RFID Reader, LED'S.

The proposed system, is designed to secure examination documents using dual-layer authentication and real-time alert mechanisms.The central controller for this system is the Raspberry pi Pico (RP 2040) microcontroller, which coordinates input from security modules and controls the output devices.

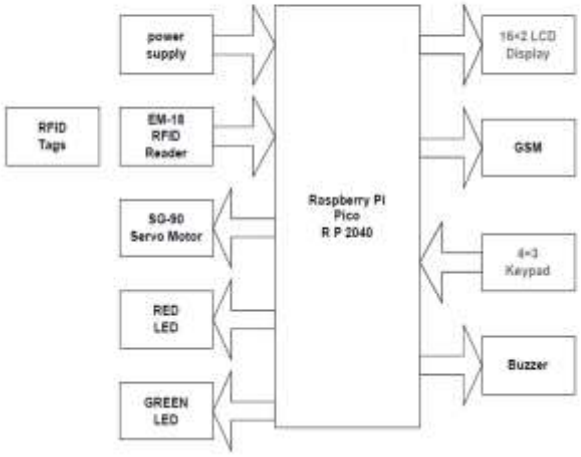


Fig -1: Block Diagram of Electronic Protection For Exam Paper Leakage

4.1 Power Supply

A regulated 5V DC power supply is provided to all
Components in the system. A Bridge Rectifier convert AC mains to DC, and an 7805 voltage regulator ensures a stable 5V output, which is distributed to devices like the microcontrollers, LCD, RFID, GSM, and others.

4.2 Input Devices

EM-18 RFID Reader with RFID tags:Used for the first level of authentication. Each college receives a unique RFID card from the university. The RFID reader scans the tag and sends the serial number to the Pico for verification.

4 X 3 keypad: Acts as the second level of security. After RFID verification, users must input the correct password, date, time using the keypad. The Pico receives and processes this input.

4.3 Output Devices

16X2 LCD Display: Provides real-time system messages such as "Enter Password", "Access Granted", "Invalid OTP", etc.

Buzzer: Sounds an alert when tampering is attempted or authentication fails.

RED LED: Indicates a failed or unauthorized attempt.

GREEN LED: Lights up when access is successfully granted.

SG-90 Servo Motor: Controls the locking/unlocking mechanism of the sealed exam paper box. It is activated only after successful authentication through RFID and password.

5. CIRCUIT DESCRIPTION

The circuit is centred around the Raspberry Pi Pico, which serves as the main microcontroller, managing communication between all peripheral components. Power is supplied through a step-down transformer that outputs AC voltage, which is then converted to DC using a bridge rectifier. This DC voltage is smoothed using filtering capacitors (1000µF, 104pF, 33pF), and regulated to 5V using a 7805 voltage regulator. This 5V DC is used to power all the components in the system.

A 16x2 LCD display is interfaced with the Pico in 4-bit mode to display system messages such as instructions and status updates. The control lines RS and EN are connected to GP2 and GP3, while the data lines D4–D7 are connected to GP4–GP7. A 4x3 matrix keypad is connected to GPIO pins GP10 to GP15, allowing the user to input a mobile number and OTP for verification.

The RFID reader (EM-18 module) communicates with the Raspberry Pi Pico via UART, using pins GP8 (TXD2) and GP9 (RXD2). It reads RFID cards operating at 13.56 MHz and sends the tag information to the Pico for verification. If the card ID matches a predefined value, access is granted.

A GSM module is connected through the UART interface using GP0 (TX) and GP1 (RX). It is used to send OTP messages to the entered mobile number and alerts in case of unauthorized tampering. Upon successful OTP verification, the system instructs the user to present an RFID card.

A servo motor connected to GP22 acts as an electronic lock. When the correct RFID card is detected, the Pico sends a signal to the servo to unlock. An alarm and buzzer, both connected to GP20, are triggered in case of tampering or invalid access attempts. These components are used to alert the user and external monitoring systems.

Finally, two indicator LEDs are connected to GP17 (Red LED) and GP18 (Green LED). These are used to visually indicate whether access has been granted (green) or denied (red). This integrated circuit ensures secure access control using a combination of time-based triggers, OTP verification, and RFID authentication.

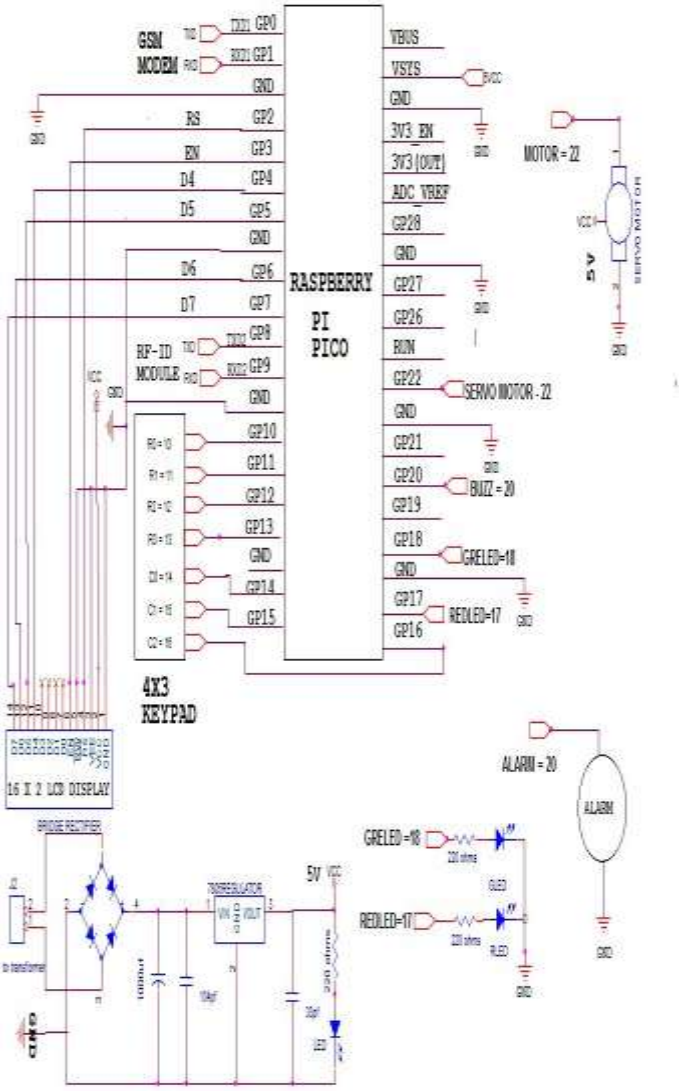
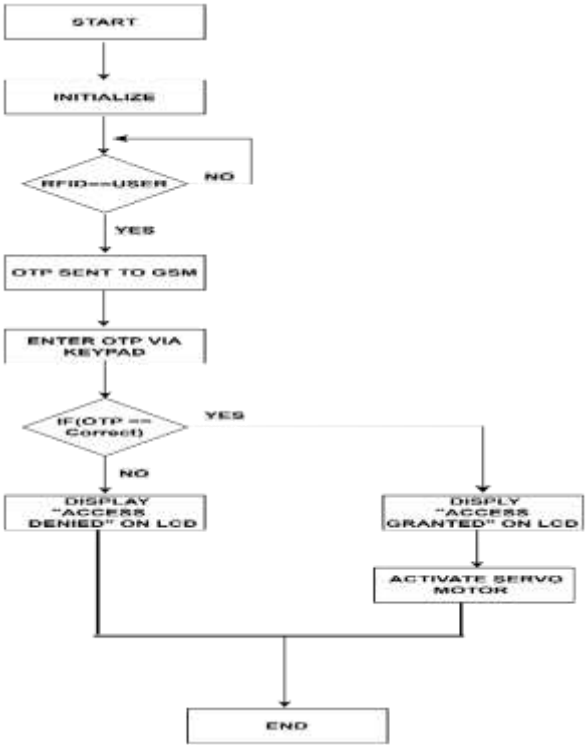


Fig -2: Circuit Diagram of Electronic protection For Exam Paper Leakage

6. FLOWCHART



7.RESULT AND DICUSSION

This prototype consists of RFID Reader, RFID Tags, Raspberry Pi Pico, Power Supply, Servo motor, 4 X 3 keypad, Buzzer, GSM module

Fig 3.1(a): Electronic Protection for Exam Paper Leakage

Fig 3.1(b) : LCD Displays the project title

LCD output during the startup of the embedded kit as shown below:

The LCD display should be show the message of the Electronic Protection for Exam Paper Leakage after the switch on the experiment kit.

Fig 3.1(c) LCD Displays Place RFID Card

LCD displaying the output during controller sending OTP to Authorized person as shown below:

The LCD Display the message sending OTP to the authorized person through GSM which is created in controller by the logic code.

Fig 3.1(d) :LCD Displays OTP Sent to Register Number

LCD displaying the output during controller asks for Enter Pass as shown below:

The OTP which is get to authorized person is loaded into the microcontroller through 4 X 3 keypad.

Fig 3.1(d) : LCD Displays Enter Pass

After entering the right OTP LCD displays the Password is correct and the servo motor will rotate in clock wise direction and comes backs to it original position.

Fig 3.1(e) LCD Displays Password Correct

Messages to authorized person from the controller as shown below: Output to authorized person during Lock of the box is open, when wrong OTP entered, when OTP mismatch messages from GSM to mobile

8 Conclusion

The Electronic Protection System against Leakage of Exam Paper was designed and implemented to ensure the serious necessity of protection for confidential academic data against improper usage and tampering. Through combining RFID authentication, OTP-based check, motion sensing, and GSM communication, the system has provided strong assurance with regard to its reliability, security, and efficacy in controlled and simulated real scenarios.

Thorough performance testing confirmed that the system constantly provided quick authentication, strong resistance to attacks, and consistent user experience with less latency. The system effectively alerted administrators about attempted unauthorized

access, recorded all action for auditing, and reported any breach or irregularity to the administrators immediately.

Although it stood tested for efficiency, the process of evaluation also found some of its limitations like reliance on the strength of the GSM network, continuous power supply, and the difficulty in scalability. Recommendations for how to overcome these limitations were put forward to improve system resilience in subsequent deployments.

The investigation of future scope also underlined the huge potential for the development of this security framework. Suggested improvements like Multi-Factor Authentication (MFA), encrypted transmission of OTP, centralized logging, Blockchain-based audit trails, and AI-powered intrusion detection systems underscore the promising directions of future development. These technologies promise to evolve the system into an even smarter, scalable, and tamper-proof solution that can address the changing security requirements of larger and more sophisticated institutions.

Finally, the project successfully completed its initial mission of providing a secure way to store examination papers with a clever, efficient, and accessible solution. Through further research, blending of future technologies, and concerted scalability activities, the system has the potential to become an upgraded platform capable of establishing new standards for security of exam papers in academic and professional testing scenarios.

9 Future Scope

The future potential of an electronic protection system for exam paper leakage is very bright, particularly in the face of growing digitization and calls for secure examination procedures. As education systems evolve into more technology-based environments, the use of microcontrollers such as the Raspberry Pi Pico can provide effective, affordable, and scalable solutions for protecting sensitive academic content. In the future, the system can be augmented with sophisticated features such as biometric authentication, real-time cloud monitoring, GPS-based tracking of question paper movement, and AI-based anomaly detection to inform authorities about suspicious behavior. In addition, as the threat of cybersecurity continues to rise, these systems can be combined with encrypted communication protocols and blockchain technology to facilitate data integrity and traceability. The small size and power consumption of the Raspberry Pi Pico render it suitable for deployment in remote and resource-scarce locations, thus enhancing the potential for implementation nationwide in urban and rural test centers.

REFERENCES

1. Ani, O. O. (2017). Exam malpractice and paper leakage: Implications for national development in Nigeria. European Scientific Journal, ESJ, 13(36),37-49.
2. 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.
3. 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.
4. K. T. Zaman, W. U. Hasan, M. M. Hillas, A. Al, M. Shaan, U. Hasan,M. Hillas, and A. Rahad, “IOT Based Question Paper Delivery Box:A Solution towards Preventing Question Paper Leakage in Public Exams of Bangladesh,” in ieeexplore.ieee.org.[Online].Available:https://ieeexplore.ieee.org/abstract/document/9057307/
5. Blazinsek, A. C. P. Elektrotechniczny, and undefined 2016,“Enhancing the accuracy of standard embedded RTC module with random synchronization events and dynamic calibration,” pe.org.pl.[Online]. http://pe.org.pl/articles/2016/11/60.pdf
6. X. Gong, Y. Wang, H. Li, J. H. . F. International, and undefined2009, “An Authentication Protocol Applied to RFID Security Systems,” in ieeexplore.ieee.org. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5283505/
7. B. Godavarthi, P. Nalajala, I. LR Teja - Internet of things, and un defined 2016, “Wireless sensors based data acquisition system using smart mobile application,” academia.edu, vol. 5, no. 1, pp.25–29, 2016. [Online]. Available: https://www.academia.edu/download/42784470/icacec2016sp06.pdf
8. P. Wankhade, S. D. I. J. Of, and undefined 2011, “Real time vehicle locking and tracking system using GSM and GPS technology-an anti-theft system,” ieeeprojectmadurai.in.http://www.ieeeprojectmadurai.in/BASE/EMBEDDEDSYSTEMS/EmbeddedSystems/357.pdf
9. E.Orji,U.Nduanya,andC. O. Latest, “Microcontroller Based Digital Door Lock Security System Using Keypad,” researchgate.net,vol.VIII,2019. [Online].
10. G. Verma, P. T. I. J. of Computer, and undefined 2010, “A digitalsecurity system with door lock system using RFID technology,”academia.edu, vol. 5, no. 11, p. 6, 2010. [Online]. Available:https://www.academia.edu/download/51636405/pxc3871334.pdf