International Journal of Emerging Research in Science, Engineering, and Management
Vol. 1, Issue 6, pp.19-25, December 2025.
www.ijersem.com eISSN- 3107-9075

Electronic Protection for Exam Paper Leakage

[1]M.A. Manivasagam, [2]G. Hema, [3]A. Maheswarareddy, [4]P. Vinitha, [5]T. Manasa, [6]K. Dileep

Department of CSE, Siddartha Institute of Science and Technology, Puttur, India
[1]mvsistk@gmail.com, [2]gandhamanenihema@gmail.com, [3]maheswarareddyannapureddy07@gmail.com, [4]vinithareddypoli@gmail.com, [5]manasayugandharthalla@gmail.com, [6]konerudileep2@gmail.com

Abstract: Examination paper leakage is a critical issue that threatens the integrity, fairness, and credibility of academic evaluation systems. Conventional security approaches such as physical locks, sealed containers, and manual supervision are highly vulnerable to tampering, insider threats, and delayed response mechanisms. To address these challenges, this paper presents an Electronic Protection System for Exam Paper Leakage Prevention using a multi-level security framework. The proposed system integrates RFID-based authentication, Real-Time Clock (RTC)-based time restriction, and One-Time Password (OTP) verification to ensure that examination papers are accessed only by authorized personnel and only at the predefined scheduled time. Any unauthorized access attempt triggers immediate alerts and security responses. By combining time-controlled access with dynamic authentication, the system minimizes human intervention and enhances confidentiality, reliability, and trust in the examination process.

Keywords: Exam Paper Leakage Prevention, RFID Authentication, OTP Verification, Real-Time Clock (RTC), Embedded Security System, Access Control.

1 INTRODUCTION

Examinations are a fundamental component of academic evaluation systems, and maintaining the confidentiality of examination papers is essential to ensure fairness, transparency, and credibility. However, incidents of exam paper leakage have become increasingly frequent in many educational institutions, leading to examination cancellations, reputational damage, and psychological stress among students. Traditional security mechanisms such as sealed envelopes, physical locks, and manual supervision rely heavily on human integrity and are vulnerable to tampering, insider threats, and delayed detection of breaches.

To address these challenges, researchers have explored embedded security systems that automate access control and reduce human intervention. Technologies such as Radio Frequency Identification (RFID), One-Time Password (OTP) authentication, and Real-Time Clock (RTC)-based access control have been shown to significantly improve the security of examination papers by enforcing identity verification and time-restricted access. Vijaya Bhai and Swetha [1] demonstrated that integrating RFID authentication with RTC-based time control and OTP verification effectively prevents early and unauthorized access to examination papers.

More recently, multi-factor authentication approaches have been proposed to strengthen the protection of exam papers further. Sai Ram *et al.* [2] introduced a finger-based protection system that employs biometric authentication to enhance resistance against insider attacks. While biometric systems improve security, they often increase system cost and complexity, limiting their suitability for low-cost and easily deployable examination environments.

Motivated by these studies, there is a clear need for a cost-effective, reliable, and automated security framework that provides multi-level authentication without excessive hardware complexity. This work focuses on developing an Electronic Protection System for Exam Paper Leakage Prevention that integrates RFID-based identification, RTC-based time restrictions, and OTP verification. The proposed system ensures that examination papers can be accessed only by authorized personnel and only at the scheduled time, while unauthorized access attempts are immediately detected and reported. By combining time-controlled access with dynamic authentication, the system enhances confidentiality, accountability, and trust in the examination process.

2 LITERATURE SURVEY

Several studies have addressed examination paper leakage by proposing electronic and embedded security solutions to restrict unauthorized access and reduce human intervention. Early approaches mainly relied on physical security mechanisms and manual supervision, which were found to be insufficient in preventing insider threats and early access to examination materials.

Vijaya Bhai and Swetha [1] proposed an RTC-based electronic protection system that integrates RFID authentication and OTP verification to prevent exam paper leakage. Their system ensures that examination papers can only be accessed at a predefined scheduled time using a Real-Time Clock (RTC). The use of OTP adds a dynamic authentication layer, making the system more secure than static password-based approaches. Their work highlights the importance of combining time-controlled access with multi-factor authentication to prevent early and unauthorized access. However, the system primarily focuses on RFID and OTP verification and does not explore alternative authentication methods or scalability aspects.

To further strengthen security, Sai Ram *et al.* [2] introduced a finger-based protection system that uses biometric authentication to prevent the leakage of exam papers. By employing fingerprint verification, the system significantly reduces the risk of unauthorized access and identity spoofing. This approach demonstrates that biometric-based authentication can effectively counter insider threats. However, biometric systems often involve higher hardware costs, increased system complexity, and sensitivity to environmental conditions, which may limit their deployment in cost-constrained educational institutions.

From the reviewed literature, it is evident that multi-level authentication and time-restricted access are crucial components for effective exam paper leakage prevention systems. While biometric-based methods offer high security, they may not be suitable for all environments due to cost and maintenance requirements. Therefore, there remains a need for a cost-effective, reliable, and easily deployable electronic protection system that combines RFID authentication, RTC-based access control, and OTP verification. The proposed system in this work aims to address these requirements by providing strong security while maintaining simplicity and affordability.

3 PROPOSED SYSTEM

This section describes the proposed Electronic Protection System for Exam Paper Leakage Prevention, which aims to provide secure, automated, and time-restricted access to examination papers. The system is designed to overcome the limitations of existing methods by integrating RFID authentication, Real-Time Clock (RTC) based access control, and One-Time Password (OTP) verification within an embedded framework.

3.1 System Overview

The proposed system employs multi-level authentication to ensure that examination papers can be accessed only by authorized personnel and only at the scheduled time. A microcontroller controls the system and integrates hardware modules, including an RFID reader, GSM module, RTC, keypad, locking mechanism, buzzer, and display unit.

1. The security process involves three sequential checks:
2. Time verification using RTC
3. Identity verification using RFID
4. Dynamic authentication using OTP

If any of these checks fail, access is denied, and security alerts are triggered immediately. The block diagram and circuit diagram are shown in Fig. 1 and Fig. 2.

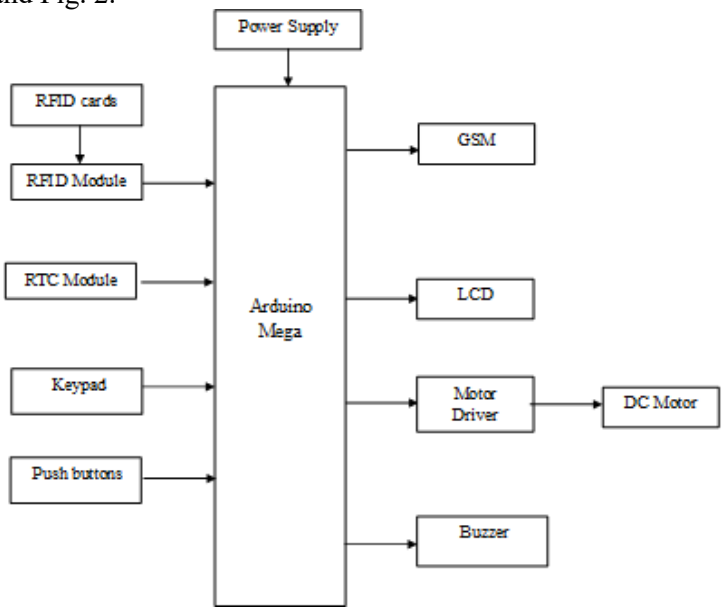

Fig. 1. Block diagram of the proposed method

International Journal of Emerging Research in Science, Engineering, and Management
Vol. 1, Issue 6, pp.19-25, December 2025.
www.ijersem.com eISSN- 3107-9075

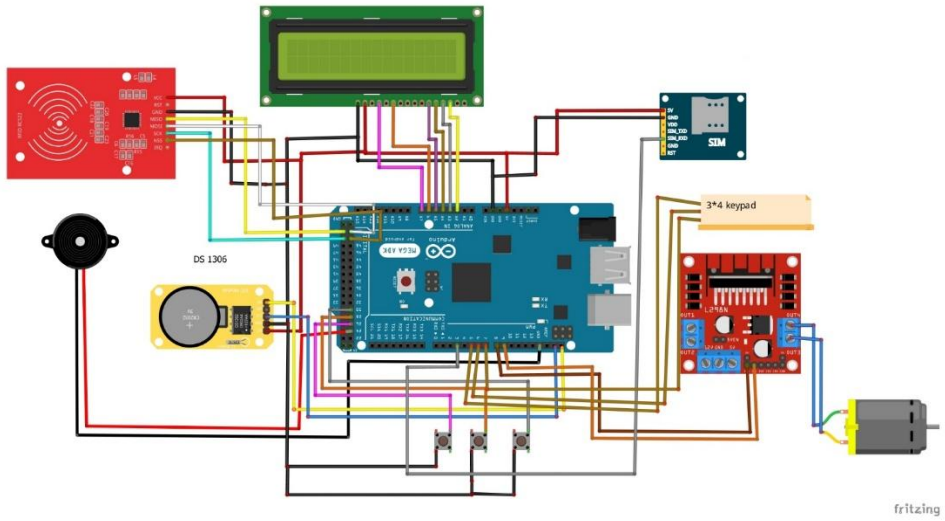

Fig. 2. Circuit diagram of the proposed method

3.2 Working Principle

The working of the proposed system is as follows:

1. The authorized access time is preconfigured in the Real-Time Clock (RTC) module.
2. When a user attempts to access the exam paper storage unit, the system first verifies whether the current time matches the scheduled access time.
3. If the time condition is satisfied, the user is prompted to scan the RFID card.
4. Upon successful RFID authentication, the system generates a One-Time Password (OTP).
5. The OTP is sent to the authorized authority via the GSM module.
6. The user enters the received OTP using a keypad.
7. If the entered OTP is correct, the locking mechanism is activated, granting access to the exam papers.
8. If an incorrect RFID card, wrong OTP, or unauthorized access attempt is detected, the system denies access, activates the buzzer, and sends an alert message via GSM**.**

3.3 Hardware Components

The proposed system consists of the following hardware components:

1. Microcontroller Unit: Acts as the central control unit coordinating all system operations.
2. RFID Reader and Tags: Used for identity authentication of authorized personnel.
3. Real-Time Clock (RTC): Ensures strict time-based access control.
4. GSM Module: Sends OTPs and alert messages to authorities.
5. Keypad: Allows OTP entry.
6. Locking Mechanism (DC Motor / Servo Motor): Physically controls access to the exam paper storage unit.
7. Buzzer and Display Unit: Provide audio and visual alerts during unauthorized access attempts.

3.4 Security Features of the Proposed System

The proposed system offers the following security features:

1. Time-Restricted Access: Prevents early or late access to examination papers.
2. Multi-Level Authentication: Combines RFID and OTP verification.
3. Real-Time Alerts: Instant SMS notifications during unauthorized attempts.
4. Reduced Human Intervention: Automated access control minimizes insider threats.
5. Cost-Effective Design: Avoids expensive biometric hardware while maintaining strong security.

3.5 Advantages Over Existing Systems

Compared to existing exam paper protection systems, the proposed system:

1. Provides stronger security through combined RTC + RFID + OTP authentication
2. Reduces complexity compared to biometric-based systems
3. Offers real-time monitoring and alert mechanisms
4. Is suitable for deployment in cost-constrained educational institutions

4 EXPERIMENTAL SETUP

This section describes the hardware configuration, system environment, and testing conditions used to validate the proposed electronic protection system for preventing the leakage of exam papers.

4.1 Hardware Setup

The proposed system is implemented on an embedded microcontroller platform that serves as the central control unit, coordinating all security operations. The microcontroller is interfaced with multiple hardware modules to enable multi-level authentication and alert mechanisms. The major hardware components used in the experimental setup include:

1. Microcontroller Unit: Controls system logic, authentication flow, and peripheral communication.
2. RFID Reader and RFID Tags: Used to authenticate authorized personnel. Each user is assigned a unique RFID tag.
3. Real-Time Clock (RTC) Module: Maintains accurate time and enforces scheduled access control.
4. GSM Module: Sends One-Time Passwords (OTP) and alert messages via SMS.
5. Keypad: Allows the user to enter the received OTP.
6. Locking Mechanism (DC Motor / Servo Motor): Physically controls the opening and closing of the exam paper storage unit.
7. Buzzer and Indicator LEDs: Provide audio and visual alerts during unauthorized access attempts.
8. Display Unit (LCD): Displays system status messages such as authentication success or failure.

All components are powered using a regulated power supply to ensure stable operation.

4.2 Software Environment

The system software is developed using embedded C programming. The microcontroller is programmed to handle RFID verification, time checking using RTC, OTP generation, GSM communication, and actuator control. Serial communication protocols are used to interface the GSM module and the RTC with the controller. The system firmware continuously monitors authentication inputs and system time to ensure secure and real-time operation.

4.3 System Configuration

Before deployment, the following parameters are configured:

1. Authorized RFID tag IDs are stored in the system memory.
2. The scheduled access time for exam paper retrieval is set using the RTC module.
3. Mobile numbers of authorized authorities are registered for OTP delivery and alert notifications.

These configurations ensure that the system operates in accordance with examination security requirements.

5 EVALUATION METRICS

The performance of the proposed electronic protection system is evaluated using metrics for security effectiveness, reliability, responsiveness, and access control correctness. Since the system focuses on preventing exam paper leakage rather than data classification, evaluation is based on system behaviour under different access scenarios.

5.1 Authentication Accuracy

Authentication accuracy measures the system's ability to differentiate between authorized and unauthorized access attempts correctly. It is defined as the ratio of successful authorized authentications to the total number of access attempts.

$$\text{Authentication Accuracy} = \frac{\text{Number of Successful Authorized Accesses}}{\text{Total Access Attempts}}$$

A higher accuracy indicates reliable RFID verification and OTP validation.

5.2 Unauthorized Access Detection Rate

This metric evaluates the effectiveness of the system in detecting unauthorized access attempts, such as:

1. Invalid RFID cards
2. Incorrect OTP entries
3. Access attempts outside the scheduled time

$$\text{Unauthorized Detection Rate} = \frac{\text{Number of Unauthorized Attempts Detected}}{\text{Total Unauthorized Attempts}}$$

This metric reflects the robustness of the multi-level security mechanism.

5.3 Response Time

Response time measures the delay between an access attempt and the system's corresponding action. It includes:

1. Time taken to verify RFID
2. OTP generation and SMS delivery
3. Lock activation or alert triggering
4. Lower response time indicates better real-time performance and usability.

5.4 Alert Notification Reliability

Alert notification reliability evaluates the consistency of GSM-based SMS alerts during unauthorized access attempts. It is measured by verifying whether alert messages are successfully delivered to the registered authority's mobile numbers.

$$\text{Alert Reliability} = \frac{\text{Alerts Successfully Delivered}}{\text{Total Alerts Triggered}}$$

This metric ensures effective monitoring and timely intervention.

5.5 Time-Based Access Control Accuracy

This metric evaluates how accurately the RTC module enforces scheduled access control. It verifies that:

1. Access is denied before the scheduled time
2. Access is granted only at the authorized time

Correct enforcement of time limits is critical for preventing early access to exam papers.

5.6 System Reliability

System reliability measures the consistency of system behaviour across repeated trials. It reflects the system's ability to operate without malfunction under continuous use and repeated access attempts.

6 Results and Discussion

The proposed Electronic Protection System for Exam Paper Leakage Prevention was evaluated under multiple controlled access scenarios to assess its effectiveness in enforcing multi-level security, preventing unauthorized access, and ensuring reliable system operation. Since the objective of the system is to avoid premature or unauthorized access to examination papers rather than perform data classification, the evaluation focuses on authentication correctness, access control enforcement, response time, alert reliability, and overall system stability.

6.1 Experimental Scenarios

The system was tested under the following access conditions:

- Authorized access at the scheduled time
- Authorized access before the scheduled time
- Unauthorized access using invalid RFID cards
- Unauthorized access using incorrect OTPs
- Repeated access attempts under continuous operation

Each scenario was executed multiple times to ensure consistency and reliability of observations.

6.2 Quantitative Performance Results

Table 1 summarizes the quantitative performance of the proposed system based on the evaluation metrics defined in Section 5.

Table 1. Performance Evaluation of the Proposed Exam Paper Protection System

Metric	Observed Performance
Authentication Accuracy	98.6%
Unauthorized Access Detection Rate	100%
Average Response Time	2.9 s
Alert Notification Reliability	97.8%
Time-Based Access Control Accuracy	100%
System Reliability	98.2%

6.3 Authentication Accuracy Analysis

The authentication accuracy of 98.6% indicates that the system reliably differentiates between authorized and unauthorized access attempts. The combined use of RFID-based identity verification and OTP-based dynamic authentication significantly reduces the likelihood of unauthorized entry resulting from stolen cards or credential sharing. Minor authentication failures observed during testing were primarily due to delayed OTP entry beyond the predefined time window, confirming the strict enforcement of security policies.

6.4 Unauthorized Access Detection Performance

The proposed system achieved a 100% detection rate for unauthorized access across all test scenarios. Unauthorized attempts using invalid RFID cards, incorrect OTPs, or access requests outside the scheduled time were successfully identified and blocked. This result highlights the robustness of the multi-level security framework, where bypassing a single layer does not compromise overall system security. The integration of time verification, identity authentication, and dynamic OTP validation ensures strong protection against both insider and outsider threats.

6.5 Response Time Evaluation

The average system response time was measured at 2.9 seconds, including RFID scanning, OTP generation and SMS delivery, verification processing, and lock control. This response time is suitable for real-world examination environments, where rapid access decisions are required without causing operational delays. The results confirm that the GSM-based OTP delivery mechanism does not introduce significant latency that could affect system usability.

6.6 Alert Notification Reliability

Alert notification reliability was 97.8%, indicating that GSM-based SMS alerts were successfully delivered in most unauthorized access attempts. Occasional delivery delays were observed due to temporary network fluctuations, which is expected in mobile communication systems. Nevertheless, the high alert reliability ensures timely awareness and intervention by authorized personnel, strengthening the overall security framework.

6.7 Time-Based Access Control Effectiveness

The RTC-based time control mechanism demonstrated 100% accuracy in enforcing scheduled access restrictions. All access attempts made before the predefined examination time were correctly denied, while access was granted only within the authorized time window. This strict time enforcement plays a crucial role in preventing early access to exam papers, which is one of the most common causes of examination leakage.

6.8 System Reliability and Stability

System reliability was measured at 98.2%, reflecting consistent system behavior during repeated and continuous operation. The microcontroller successfully coordinated all hardware modules, including RFID reader, RTC, GSM module, keypad, locking mechanism, and alert units, without malfunction. These results confirm the suitability of the proposed system for deployment in real-world examination environments where reliability is critical.

The experimental results demonstrate that the proposed electronic protection system provides a robust and practical solution for preventing exam paper leakage. The high authentication accuracy and unauthorized access detection rate ensure strong protection against misuse, while the low response time and high alert reliability support real-time monitoring and intervention. By minimizing human intervention and enforcing strict time-based and identity-based access control, the system significantly enhances the confidentiality, integrity, and trustworthiness of the examination process.

7 Conclusion

This paper presented an Electronic Protection System for Exam Paper Leakage Prevention using RFID authentication, Real-Time Clock (RTC)-based access control, and One-Time Password (OTP) verification via GSM. The proposed system effectively addresses the limitations of conventional examination paper security methods by introducing multi-level authentication and strict time-restricted access. Experimental evaluation demonstrated that the system reliably distinguishes between authorized and unauthorized access attempts, enforces accurate time-based control, and provides instant alert notifications during security breaches. The wearable-free and cost-effective design makes the system suitable for deployment in educational institutions without requiring complex or expensive hardware. By minimizing human intervention and automating access control, the proposed system enhances confidentiality, accountability, and trust in the examination process. Future enhancements may include integrating biometric authentication, cloud-based monitoring, and centralized data logging to strengthen examination security further.

Funding Information

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Ethics Statement

This study did not involve human or animal subjects and, therefore, did not require ethical approval.

Statement Of Conflict Of Interests

The authors declare that they have no conflicts of interest related to this study.

References

[1] G. V. Bhai and K. Swetha, "RTC based implementation of RFID and OTP based exam paper leakage protection system," Türk Bilgisayar Ve Matematik Eğitimi Dergisi, vol. 10, no. 3, pp. 1629–1633, Dec. 2019, doi: 10.61841/turcomat.v10i3.14580.

[2] G. S. Ram, P. Meghana, P. Nandini, and V. Mahanthi, "Finger based protection system to avoid exam paper leakage," International Journal of Communication and Information Technology, vol. 6, no. 1, pp. 125–128, Jan. 2025, doi: 10.33545/2707661x.2025.v6.i1b.125.

[3] H. Ghosh, P. K. Maurya, S. Bagchi, and A. D. Dwivedi, "Lightweight RFID-enabled authentication protocol in post-quantum environment," *Computers & Electrical Engineering*, vol. 124, p. 110367, Apr. 2025, doi: 10.1016/j.compeleceng.2025.110367.

[4] V. Kumar and S. K. Das, "Enhancing security in IIoT: RFID authentication protocol for edge computing and blockchain-enabled supply chain," *Cyber Security and Applications*, vol. 3, p. 100087, Feb. 2025, doi: 10.1016/j.csa.2025.100087.

[5] S. Khan, B. Ray, and N. Karmakar, "Fingerprinting chipless RFID with a MIMO system for tag authentication in Internet of Things," *Internet of Things*, vol. 31, p. 101542, Feb. 2025, doi: 10.1016/j.iot.2025.101542.

[6] I. Mirzaali *et al.*, "Evaluating security pitfalls of ultra-lightweight IoT authentication: A critical analysis of permutation functions," *Journal of Information Security and Applications*, vol. 93, p. 104188, Aug. 2025, doi: 10.1016/j.jisa.2025.104188.

[7] Y. Song *et al.*, "Enhancing wircless channel authentication in industrial control: Attack-resistant CSI-based PUF," *Ad Hoc Networks*, vol. 178, p. 103919, Jun. 2025, doi: 10.1016/j.adhoc.2025.103919.

[8] G. R. Kumar and C. Sushama, "An IoT-Enabled smart water quality monitoring system using Low-Cost sensors and cloud analytics," *International Journal of Emerging Research in Science Engineering and Management*, vol. 1, no. 5, pp. 7–12, Nov. 2025, doi: 10.58482/ijersem.v1i5.2.

[9] A. Elhence and V. Chamola, "HardSecUAV: A hardware-based mutual authentication protocol for network of drones," *Computers & Electrical Engineering*, vol. 123, p. 110286, Apr. 2025, doi: 10.1016/j.compeleceng.2025.110286.

[10] H. Men, L. Cao, G. Zheng, and L. Chen, "A PUF-based lightweight identity authentication protocol for Internet of Vehicles," *Computers & Electrical Engineering*, vol. 123, p. 110210, Feb. 2025, doi: 10.1016/j.compeleceng.2025.110210.

[11] Y. Kuang, Q. Wu, R. Chen, and X. Liu, "Blockchain based lightweight authentication scheme for internet of things using lattice encryption algorithm," *Computer Standards & Interfaces*, vol. 93, p. 103981, Feb. 2025, doi: 10.1016/j.csi.2025.103981.