WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Controller Based Paper Leakage System

Darpan Kulkarni, Mansi Avhad, Ganesh Chaughule, Yashashri Bhadane

Department of Electronics & Telecommunication Engineering

ABSTRACT-

Examination paper leakage has been a major concern in educational institutions, leading to loss of credibility, academic dishonesty, and compromised evaluation standards. The Controller-Based Secure Exam Paper Leakage Prevention System aims to provide a technological solution that ensures confidentiality and integrity of examination materials. The proposed system uses a microcontroller-based secured network to automate paper distribution, encryption, and timed access control.

Exam papers are securely transmitted from the controller to authorized nodes (exam centers or digital lockers) only during a defined time window. This approach integrates embedded systems, cryptographic algorithms, and IoT-based authentication mechanisms to minimize human involvement and eliminate vulnerabilities. The system offers a reliable, automated, and costeffective way to protect exam content and restore faith in the examination process.

Index terms- Lock Mechanisms; lithium-ion battery; GSM module; STM 32 Microcontroller

1. Introduction :

In the current educational environment, maintaining the confidentiality of examination papers is critical. However, traditional methods such as manual printing, storage, and distribution have proven to be vulnerable to leaks, manipulation, and unauthorized access. Several incidents of question paper leaks have occurred globally, causing severe academic and administrative challenges. To address this issue, this project proposes a Controller-Based Secure Exam Paper Leakage Prevention System that leverages the capabilities of embedded controllers (e.g., Arduino or Raspberry Pi), secured data transmission, and authentication modules.

The system ensures that exam papers are stored in encrypted form and can only be accessed through authorized hardware units at a specific scheduled time, controlled by a central unit. The solution combines hardware and software elements to automate secure exam paper delivery, reducing human interference and improving reliability. The system's real-time control features make it highly adaptable for universities, schools, and government examination authorities.

2.1 Literature Review :

The persistent issue of examination paper leakage continues to damage the integrity and credibility of educational and recruitment systems worldwide. Traditional preventive measures such as sealed envelopes, manual supervision, and strict administrative protocols have repeatedly failed due to human error, insider collusion, and physical tampering. In response, researchers have increasingly turned toward controller-based systems that embed microcontrollers, sensors, cryptography, and communication modules to create secure, automated locks for exam materials. The literature in this domain spans hardware- based designs, IoT extensions, multi-factor authentication, blockchain integrations, and hybrid models combining physical and digital safeguards. Mamilla Sirisha and Neelam Syamala (2018) propose an early electronic security framework for preventing exam paper leaks using an ARM-based "Electronic Control Box" that houses the question papers. Their design integrates an RFID module, keypad interface, electromagnetic lock, real-time clock (RTC), and GSM modem. The box opens only if an authorized RFID credential or PIN is entered within a permitted time window. Deviations from expected behavior trigger SMS alerts to the central authority (e.g., university) about possible tampering or unauthorized access attempts. Their work represents a practical baseline for combining microcontroller control, scheduled access, and remote notification. Building on that architecture, Rajitha et al. present an RFID + OTP + RTC scheme wherein a valid RFID tag must be augmented with a one-time password (OTP) entered via keypad. The OTP is generated dynamically and expires after a short period, reducing the risk of credential reuse or compromise. The RTC ensures that access is granted only during a predefined window, and logging of attempts is maintained. This design strengthens the authentication process by introducing credentials.

2.2 Review of Related Literature

2.2.1 Linkage Mechanisms and Their Applications.

Linkage mechanisms are essential components in many mechanical and robotic systems, transforming motion and force through connected rigid links and joints. According to Singh et al. (2019), four-bar and six-bar linkages are among the most commonly used configurations in industrial and robotic applications due to their ability to convert rotary motion into linear or complex motion paths. **Kumar and Patel (2021)** emphasized that proper kinematic modeling of linkages is vital for ensuring accurate motion and reducing vibration and wear in automated machines.Linkage-based systems are also used in assistive and rehabilitation devices. **Mishra et al. (2022)** reviewed various linkage-based gait rehabilitation devices, highlighting how different linkage topologies affect motion patterns and patient comfort. These studies underline the importance of linkage geometry and motion analysis in designing efficient mechanisms before control integration.

2.2.2 Control Systems for Linkage Mechanisms.

With the advancement of automation, linkage systems are often integrated with controllers to achieve precise and adaptive motion. Conventional controllers such as **Proportional–Integral–Derivative (PID)** remain popular for their simplicity and robustness (**Ali & Rahman, 2020**). However, for systems affected by nonlinearities or uncertainties (e.g., joint clearance, load variation), advanced control strategies such as **fuzzy logic**, **neural networks**, and **adaptive control** have been proposed (**Zhao et al., 2021**).For instance, **Zhang and Liu (2018)** developed a neural-network-based intelligent controller for a linkage mechanism with clearance, showing improved stability and reduced steady-state error compared to traditional PID control. Similarly, **Rahim et al. (2020)** applied sliding-mode control to a five-bar linkage manipulator, achieving high tracking accuracy under uncertain operating conditions.

2.2.3 Integration of Linkage Design and Control.

Recent studies have stressed the need for the **co-design** of the mechanical linkage and the controller rather than treating them as separate subsystems. **Tanaka etal. (2022)** demonstrated that optimizing linkage geometry and control parameters simultaneously leads to smoother motion and lower energy consumption. In industrial automation, **Chengetal. (2019)** used a PLC-based controller for an automatic steering linkage system, proving that real-time control enhances production efficiency and repeatability. In robotic applications, **Kaur and Bhatia (2021)** designed a six-linkage robotic arm with a robust controller, reporting high precision in position control and low overshoot. Such studies suggest that hybrid approaches—combining model-based and intelligent control—can offer significant performance improvements.

2.24 Challenges and Research Gaps.

Although many controller-based linkage systems have been studied, several challenges remain. Accurate dynamic modeling of multi-link mechanisms is complex, particularly when flexibility, friction, and backlash are present (**Lee et al., 2020**). Moreover, most research focuses on ideal laboratory setups, while fewer studies address implementation in industrial or field environments where disturbances are unavoidable. There is also a need for **standardized testing and evaluation metrics** for linkage-controller systems to enable fair comparison among different designs. Future research should focus on **adaptive, self-learning controllers** that can automatically tune themselves for varying load and environmental conditions, as well as on cost-effective sensor integration for feedback and diagnostics.

2.2.5 Summary

The literature shows a continuous evolution from simple mechanical linkages controlled by basic feedback mechanisms to advanced, intelligent, and adaptive systems. Researchers agree that coupling mechanism design with control strategy results in better performance and reliability. However, issues related to modeling accuracy, uncertainty management, and system cost remain open for further investigation.

3. Block Diagram :

Components and Operation:

1. **Power Supply**:

Converts AC mains (230V) to a stable DC voltage (usually 5V or 3.3V) suitable for the ESP328, sensors, and modules.

2. **ESP328 Microcontroller Unit:**

Reads data from keypad, RFID reader, and MEMS sensor**.** Controls output devices (LCD, motor, buzzer, GSM). Makes logical decisions based on programmed conditions (e.g., unlocking a door if correct RFID or keypad input is provided).

3. **Keypad:**

User enters a PIN. The keypad sends corresponding key signals to the ESP328. The controller verifies if the input matches the stored password.

4. **RFID Tag and RFID Reader:**

The RFID reader reads the unique ID stored in the RFID tag. Sends the ID to the ESP328. The controller checks if the ID matches a stored authorized ID.

5. **MEMS Sensor (Micro-Electro-Mechanical System Sensor):**

If abnormal movement or tampering is detected, it sends a signal to the ESP328. The controller may trigger an alarm or send an alert via GSM. Detects vibration, motion, or orientation changes.

6. **LCD (Liquid Crystal Display)**

The ESP328 sends display data (e.g., “Access Granted”, “Invalid Tag”, “Enter Password”). LCD shows these messages to the user.

7. **DC Motor:**

Controlled by L293D based on commands from the ESP328. Rotates in either direction to lock/unlock.

8. **Buzzer:**

Controlled by ESP328. Beeps when access is denied, when an error occurs, or as an alert in case of tampering.

3.1 Working Principle

1. System Initialization

a) When the system is powered on, the power supply provides stable DC voltage to all connected components.

b) The ESP328 microcontroller initializes all peripherals RFID reader, keypad, LCD, GSM module, and motor driver.

c) The LCD displays a welcome or ready message (e.g., “System Ready” or “Swipe Card / Enter PIN”).

2. Authentication Process:

a) The user presents an RFID tag near the RFID reader. The reader scans the unique ID stored in the tag and sends it to the ESP328.

b) The controller compares the scanned ID with the IDs stored in its memory. The controller compares the scanned ID with the IDs stored in its memory.

3. Access Control:

a) If unauthorized The ESP328 sends a control signal to the L293D motor driver. The L293D drives the DC motor, which operates the door lock (opens or closes).

b) The buzzer will start sounding, indicating an intrusion.

c) Simultaneously, the GSM module will send a security alert SMS to the registered mobile number, informing the owner of the potential security breach.

4. Security and Alerts:

a) If unauthorized access is detected, the system will trigger both a physical and digital alert:

b) The **buzzer** will start sounding, indicating an intrusion.

c) Simultaneously, the **GSM module** will send a security alert SMS to the registered mobile number, informing the owner of the potential security breach

5. System Feedback :

a) If unauthorized access is The LCD displays system status at each stage.

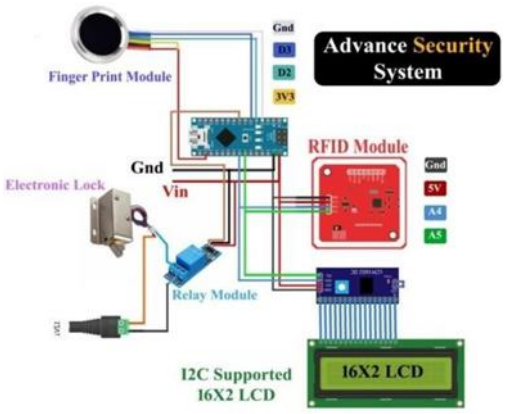
b) The buzzer will This ensures the user is informed of system operations in real time.

6. Reset and Standby :

a) The system runs After an operation (door open/close), the system resets and returns to standby mode.

b) It waits for the next RFID or keypad input for a new authentication cycle.

3.2 Circuit Diagram



4. Conclusion :

The Controller Based Secure Paper Leakage Prevention System effectively addresses the serious issue of paper leaks by integrating encryption, authentication, and monitoring at the hardware level. By automating security and limiting access, the system ensures fair and transparent examination processes. This project successfully implements a secure paper storage and tracking system to prevent leakage. By combining modern technologies like GSM, GPS, RFID, and biometric authentication with a microcontroller, the system provides a robust solution for maintaining exam confidentiality. It ensures only authorized personnel can access the exam papers while keeping authorities informed of the box's location. Such a system can significantly enhance the security and trust in the examination process