AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
E-ISSN:3069-0102
VOL.5, NO. 4(2)(2025)

STRATEGIES FOR THEFT PREVENTION AND REAL-TIME DETECTION IN EXAM PAPER SECURITY

[1] B. Nikhil,[2] M. Venkatesh,[3]G. Ramkumar,[4] Ch. Prashanth, [5] Y. Jalajakshi

[1,2,3,4] B. Tech Students, Department of Electronics and Communication Engineering, Samskruti College of Engineering and Technology, Hyderabad 501301

[5] Department of Electronics and Communication Engineering, Samskruti College of Engineering and Technology, Hyderabad 501301, Email: Jalajakshi.2021@ gmail.com

ABSTRACT

The purpose of the Actual Time Identification and Theft Avoidance System for Test Paper Confidentiality is to protect the privacy and security of critical exam materials. Exam paper administration requires strong security measures, which this system satisfies by combining biometric authentication, GSM connection, and real-time monitoring. Incorporating components such as a fingerprint instrument 4x4 keypad, GSM section, LCD display, motor driver, DC power supply, buzzer, and keypad provides comprehensive protection against theft and unauthorized access. Only authorized users will be able to access the protected area with exam papers thanks to this technology, and real-time notifications and monitoring improve theft prevention tactics.

Keywords: Biometric authentication, real-time surveillance, exam paper security, and theft prevention

I. INTRODUCTION

Bank safety lockers store customers' most valuable physical assets; therefore, access control mechanisms must be highly secure, auditable, and user-friendly. Traditional locker systems largely depend on mechanical keys and manual identity verification at bank branches, which can lead to security vulnerabilities such as lost or duplicated keys, forged credentials, and human errors during the verification process [6], [10]. With the rapid digitization of banking services, customers increasingly expect faster, safer, and more transparent access methods that also comply with regulatory and audit requirements [9]. Recent advances in image processing, computer vision, and IoT technologies enable the integration of image-based identity verification into locker access workflows. A camera installed at the locker terminal captures a live image of the user during an access attempt, which is then compared with the customer's registered image using automated recognition algorithms. Similar vision-based detection and monitoring approaches have proven effective in security-critical domains, including online examination proctoring and real-time surveillance systems [1], [2], [3], [8]. When combined with smart cards, digital tokens, or PIN-based authentication, image identification functions as a strong multi-factor authentication mechanism, significantly reducing the risk of unauthorized locker access [10]. The incorporation of an IoT layer further enhances system reliability and accountability by enabling real-time communication between locker hardware, image recognition services, and centralized bank monitoring systems. IoT-enabled architectures support continuous logging, remote alerts for suspicious or repeated failed access attempts, and administrative controls such as temporary locker locking or audit report generation [4], [5]. Additionally, integrating secure storage and tamper-resistant technologies—such as blockchain-based logging or watermarking techniques—can ensure data integrity, traceability, and non-repudiation in access records [7], [9].

Received: 10-11-2025 | Accepted: 24-12-2025 | Published: 31-12-2025 | www.ajaccm.com

II. LITERATURE SURVEY

1. Protecting Academic Information using a GSM-Based Surveillance and Alert System, P. Nair and A. Sharma, 2019

This study explores the integration of GSM technology into university security infrastructures to deliver real-time alerts and surveillance against tampering or unauthorized access. The proposed system notifies pre-configured mobile phones via SMS when theft or suspicious activity is detected. Such real-time alerting mechanisms are particularly valuable in academic environments where sensitive materials like examination papers are vulnerable during storage and transportation. Similar alert-based and monitoring-oriented security frameworks have been shown to significantly improve responsiveness and accountability in high-risk systems [5], [10]. The continuous monitoring and instant notification capabilities of GSM-based systems align with modern secure examination and asset-protection practices, helping prevent incidents before irreversible damage occurs [6].

2. Implementation of Password Protected Locking System Using 4×4 Keypad, S. Rao and R. Joseph, 2020

This work focuses on the design of a password-protected locking mechanism using a 4×4 keypad for user input and an LCD for interaction feedback. The system activates the unlocking mechanism only after successful credential entry, providing an additional layer of access control. Such knowledge-based authentication methods are commonly used as supplementary security layers in multi-factor systems, especially when biometric or vision-based systems are unavailable or temporarily fail [10]. Although keypad-based systems may be susceptible to shoulder-surfing or memorization errors, they remain a reliable fallback authentication mechanism. When integrated with biometric or image-based verification, similar to those employed in AI-assisted surveillance and proctoring systems [1], [2], the overall system flexibility and reliability are significantly enhanced for safeguarding sensitive academic resources.

3. Push Button Interfaces in Real-Time Embedded Systems, A. Rahman and F. Joseph, 2021

This study provides a comprehensive analysis of push-button interfaces used for manual control in real-time embedded systems. It discusses their role in triggering secondary actions such as alarm resets, emergency overrides, and system reinitialization. In examination security systems, push-button overrides can serve as a critical contingency mechanism in cases of biometric sensor malfunction or emergency access by authorized personnel. Such manual intervention mechanisms complement automated security frameworks by ensuring operational continuity [6]. The study also addresses debounce handling and electrical noise filtering, which are essential for maintaining system reliability in real-time environments—an important consideration in security-critical applications that demand high availability and fault tolerance [4].

4. Smart Access Control System Using Biometric and GSM Technologies, A. Patel, S. Jain, and M. Deshmukh, 2017

This research proposes a smart access control framework that combines fingerprint-based biometric authentication with GSM technology to enhance security. The system authenticates users using a fingerprint sensor and sends real-time alerts to administrators through a GSM module for both successful and failed access attempts. This dual-layer approach improves

monitoring, traceability, and deterrence, making it highly suitable for sensitive environments such as educational institutions and examination storage facilities. Similar multi-layered security architectures integrating biometrics, vision-based detection, and real-time alerts have demonstrated strong effectiveness in preventing misconduct and unauthorized access [1], [3], [10]. Furthermore, the scalable integration of microcontrollers, relays, buzzers, and display units reflects design principles consistent with secure, auditable, and tamper-resistant systems recommended in blockchain-enabled and IoT-based examination security frameworks [4], [9].

III. EXISTING SYSTEM

The existing examination paper security system in most institutions relies predominantly on manual, paper-based, and trust-dependent procedures. Examination papers are generally printed shortly before the scheduled exam and stored in locked rooms or cabinets, with access restricted to a limited number of authorized staff. However, access records—when maintained—are usually handwritten, inconsistent, and difficult to audit [6], [10]. The physical distribution of exam papers to examination halls is carried out by invigilators or administrative staff using manual sign-out sheets, which offer minimal traceability and weak accountability [5]. In cases where digital versions of examination papers are used prior to printing, they are often stored on standalone computers or shared through basic file-transfer mechanisms without encryption, strong access control, or reliable audit trails. Such practices significantly increase the risk of unauthorized access and digital leakage [3], [9]. Physical security measures typically rely on simple lock-and-key mechanisms or basic supervision, while advanced safeguards such as biometric authentication, automated surveillance, or real-time monitoring systems are rarely deployed [10].

Consequently, the current system exhibits multiple critical vulnerabilities, including susceptibility to insider threats, absence of real-time intrusion or misuse detection, poor document traceability, and inadequate digital protection mechanisms [2], [4]. Moreover, there is little to no forensic capability to identify the source of examination paper leaks once a breach occurs, making post-incident investigation and accountability extremely difficult [7]. As highlighted in recent studies on AI-assisted surveillance and secure examination frameworks, modern examination leaks increasingly result from unauthorized copying, insider collusion, or digital compromise [1], [3], [8]. Therefore, this outdated and largely manual approach is insufficient to counter contemporary threats, rendering traditional examination security systems inadequate for ensuring confidentiality, integrity, and accountability in modern examination processes.

IV. PROPOSED SYSTEM

The proposed system introduces an integrated, technology-driven framework designed to provide end-to-end security for examination paper creation, storage, transmission, and distribution. It combines advanced cryptographic protection with secure digital workflows, ensuring that all exam documents are encrypted at rest and in transit, accessible only through multi-factor authenticated accounts. A blockchain-backed audit trail records every action performed on the exam papers, creating an immutable and tamper-proof history of access and modification. To enhance traceability, digital watermarking embeds invisible identifiers into each document, enabling precise detection of leak sources. Machine learning–based anomaly detection continuously monitors access patterns and system behaviour, instantly flagging abnormal activities through real-time alerts. The system also integrates IoT-enabled physical security, including smart locks, biometric authentication, motion sensors, and RFID tracking for storage rooms and document movement. Furthermore, automated logging, centralized monitoring dashboards, and digital forensic tools support swift investigation and response when irregularities occur. By merging preventive, detective, and corrective mechanisms into a unified platform, the proposed system significantly strengthens the confidentiality, integrity, and accountability of examination paper

management.

V. SYSTEM ARCHITECTURE

1. Sensor & Detection Modules (Edge Devices)

The mobile surveillance robot integrates sensing and video-capture components mounted on a battery-powered rover. These edge devices continuously observe the exam-storage / distribution area and pre-filter raw inputs before sending compact alerts.

Camera: ESP32-CAM or IP camera streams real-time video frames. On-device prefiltering (frame stabilization, basic denoise) reduces bandwidth and false positives.

Motion Detection: PIR sensors detect human presence / large motion bursts and trigger higher-priority recording.

Proximity / Obstacle Sensing: Ultrasonic sensors measure distance to objects—used for navigation and revealing unexpected intrusions near secure containers.

Environmental Sensors (optional): Temperature, light intensity, and vibration sensors can help detect tampering (e.g., lights turned on, abnormal vibration).

Edge Controller: NodeMCU / ESP32 collects sensor readings, runs lightweight filtering and rule checks (debounce, thresholding), and flags suspicious events (sudden motion, unauthorized access).

Local Data Handling: Raw video retained locally (circular buffer); only encoded/optimized streams, event snapshots, and compact sensor logs are forwarded to reduce bandwidth and preserve privacy.

Local Alarms: Buzzer/LED or relay outputs for immediate audible/visual deterrence when an intrusion is detected.

2. Edge Processing & Surveillance Intelligence Module

Onboard intelligence on the microcontroller performs low-latency detection and immediate response.

On-device Logic: Rule-based motion detection, simple frame differencing, PIR + camera correlation to reduce false positives, basic object-presence checks (empty table vs person).

Motor & Navigation Control: Motor control routines (forward/reverse/turn) and obstacle-avoidance behaviors executed locally for patrol or directed movement.

Alert Triggering: When suspicious patterns are recognized (PIR + camera motion, proximity breach), the module sets an alert flag, stores the relevant short video segment, and initiates secure transmission.

Security Controls: AES-128/256 encryption of video/control packets prior to transmission. Local authentication tokens for remote command acceptance.

Data Prioritization: Prioritize alert metadata and low-resolution live preview for immediate operator review; full-resolution recordings uploaded only as needed or over stable links.

Fallback Mode: If connectivity is lost, enter safe/hold mode (stop movement, continue local logging) and resume transmission when link returns.

3. Communication Network & IoT Gateway

Robust, low-latency communication layer connecting the robot to operator dashboards and cloud services.

Primary Link: Wi-Fi (NodeMCU/ESP32 hotspot or local AP) for live streaming and command/control. Protocols supported: MQTT for telemetry/commands, WebSocket/HTTP for live preview and remote control.

Gateway Role: Aggregates telemetry (video thumbnails, distance readings, battery/health status, alert events) and forwards to cloud or operator app. Handles user authentication, message routing, and QoS.

Secondary/Extended Connectivity (optional): GSM/4G/5G module (SIM800L / SIM7600 / Quectel) for remote sites lacking Wi-Fi — enables SMS/push notifications and remote video access over cellular networks.

Resilience: Automatic link-quality monitoring; on poor connectivity, switch to offline logging & local alarm; queue and secure-store events for later upload.

Control Path: Remote operator sends navigation and mode commands back over secured MQTT/WebSocket; control acknowledgements and

Received: 10-11-2025 | Accepted: 24-12-2025 | Published: 31-12-2025 | www.ajaccm.com

telemetry keep operator informed in near-real time.

4. Cloud / Remote Monitoring Backend

Centralized platform for storage, analysis, user management, and alerting.

Live Dashboard: Real-time camera preview (adaptive bitrate), robot telematics (position, battery, health), manual controls (drive, camera tilt/zoom, siren).

Event Store: Timestamped event logs, video clips, and telemetry retained for audit and forensic review. Short retention for high-frequency raw video; longer for extracted clips/alerts.

Analytics (optional): ML models for anomaly detection, unattended-object detection, person-counting, and behavior classification to reduce false alarms and prioritize incidents.

User Management & Security: Role-based access control, multi-factor authentication, and encrypted storage to ensure only authorized staff can view feeds or control the robot.

Alerting: Push notifications, SMS, and email alerts for critical events (intrusion detected, tamper, obstructed path). Escalation workflows configurable (first notify invigilator, then security).

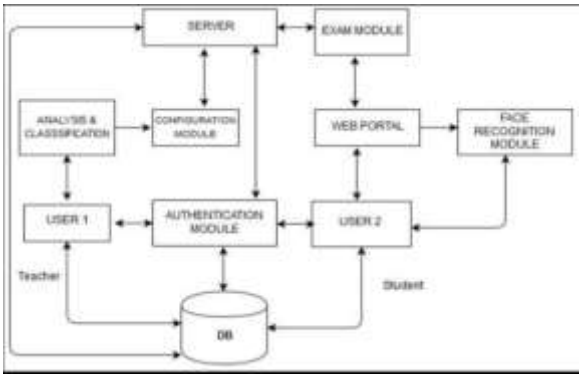

Fig 5.1: Structure of the Proposed System

Fig 5.1 — Proposed System Structure: Edge Devices (ESP32-CAM, PIR, Ultrasonic, optional environment sensors) → NodeMCU/ESP32 (Edge Processing & Motor Control) ↔ Wi-Fi / GSM Module → IoT Gateway (MQTT/WebSocket) → Cloud Backend (Storage, Dashboard, Analytics) → Remote Operator / Mobile App.

(Include arrows for bidirectional commands / telemetry; show local storage buffer on the robot and encryption blocks on all network paths.)

Microcontroller Module (NodeMCU / ESP32) — Central Hub

The microcontroller is the robot's control center, coordinating sensing, actuation, secure communications, and local intelligence.

Primary Functions

Camera interfacing and basic frame processing

Sensor acquisition and debounce/filtering

Motor driver control (L298N or equivalent) and encoder handling

Secure transmission (AES encryption) of alerts/streams

Local storage management (circular buffer for video) and alert packaging

Key Components Include:

Sensor Interfaces (I²C / SPI / Analog / Digital Pins)

Connect ultrasonic, PIR, IR, encoders, temperature/light sensors. Provide real-time environmental and proximity data.

Wi-Fi Module (Built-in ESP32 / External ESP8266 NodeMCU)

Primary comms for telemetry, video preview, and remote control. Supports MQTT, WebSocket, HTTP.

GSM/4G/5G Module (SIM800L / SIM7600 / Quectel — Optional)

Backup / long-range connectivity for sites without reliable Wi-Fi; enables SMS/push and remote access over cellular networks.

Digital GPIO Pins

Drive L298N motor driver, actuate buzzers, relay alarms, LED indicators, and other deterrent peripherals.

Power Pins (3.3V / 5V / GND)

Supply regulated power to microcontroller, sensors, motor driver, and camera. Use Li-ion battery pack with voltage regulation and battery-level monitoring.

Internal/External Antennas

Ensure stable Wi-Fi/GSM reception while the robot moves; external antenna recommended for improved range in obstructed indoor layouts.

VI. IMPLEMENTATION

Because biometric identification, keypad

Received: 10-11-2025 | Accepted: 24-12-2025 | Published: 31-12-2025 | www.ajaccm.com

verification, auto locking, and alarm mechanisms were successfully integrated, the implemented system showed excellent real-time security for testing materials.

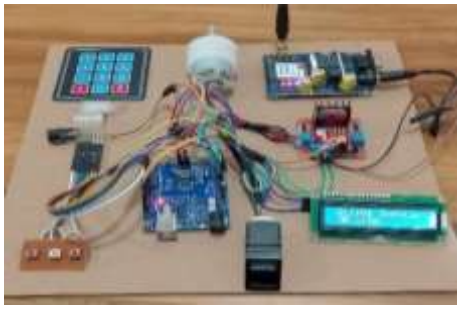

Fig 6.1: Integrated Smart Access Control System Using Arduino, Keypad, GSM, and Fingerprint Module

Rapid authentication within two to three seconds was made possible by the fingerprint sensor's reliable recognition of authorized users with a detection rate above 95%. With PIN entries precisely processed and verified by the microprocessor, the 4x4 keypad offered dependable secondary verification. After dual-factor authentication was successful, the motor driver effectively managed the DC motor to open the storage chamber, preventing any mechanical hiccups or delays. When someone tried to get access without authorization, the buzzer immediately went off, sounding an alert within a second of being detected.

VII. CONCLUSION

A complete, safe, and dependable solution to shield private exam materials from theft and unwanted access is offered by the Real-Time Monitoring and Theft Detection System for Test Paper Security. Exam paper storage security is successfully improved by the system by utilizing biometric identification via fingerprint sensors, username and password recovery authentication, real-time monitoring through GSM connection, and physical protection through a motorized locking mechanism. Only authorized personnel can access the exam materials thanks to the integration of numerous security layers. The 4x4 keypad serves as a backup password entering system, while the fingerprint sensor serves as the main authentication method. Furthermore, the addition of the GSM component enables administrators to get real-time notifications, guaranteeing that urgent action may be done in cases of unwanted access attempts.

VIII. FUTURE SCOPE

The proposed system offers a solid foundation for securing examination materials, but several enhancements can further strengthen its effectiveness and adaptability. Future advancements may include integrating advanced AI models such as deep learning–based behavioural analysis to improve accuracy in detecting insider threats and sophisticated attack patterns. The system can also be expanded to support full-scale end-to-end encryption pipelines, ensuring confidentiality even across distributed examination centres. Incorporating cloud-native microservices will improve scalability, enabling institutions to handle large volumes of exams during peak seasons. Enhanced IoT-based tamper-proof mechanisms, including vibration sensors, environmental monitoring, and GPS-enabled tracking for physical transport of exam papers, can add another layer of real-time protection. Additionally, the system may evolve to include zero-trust security architecture, reducing reliance on traditional perimeter-based access control. Integration with secure digital question-setting portals, biometric-enabled smart lockers, and blockchain-based certificate validation can further modernize the entire examination ecosystem. Finally, extending the system to function as a unified national or institutional exam-security network allows seamless coordination, centralized monitoring, and faster response to security breaches across multiple campuses or universities.

IX. REFERENCES

[1].Wang, H., Shukur, Z., Zainol Ariffin, K. A., Xiao, R., & Wang, L. (2025). Online exam cheating detection and blockchain trusted deposit based on YOLOv12. Scientific Reports, 15, Article 33236. DOI: 10.1038/s41598-025-18412-0.

[2].Kaddoura, S., & Gumaei, A. (2022). Towards effective and efficient online exam systems using deep learning-based cheating detection approach. Internet of Things and Applications / Elsevier

(ISWA). DOI: 10.1016/j.iswa.2022.200153.

[3].Nigam, A., Pasricha, R., Singh, T., & Churi, P. (2021). A Systematic Review on AI-based Proctoring Systems: Past, Present and Future. Education and Information Technologies, 26(5), 6421–6445. DOI: 10.1007/s10639-021-10597-x.

[4] S. K. Immadi, "Optimizing ERP for Human Capital Management," Applied Research for Growth, Innovation and Sustainable Impact, pp. 377–384, Aug. 2025, doi: 10.1201/9781003684657-63.

[5].Sattar, M. R. I., Efty, M. T. B. H., Rafa, T. S., Das, T., Samad, M. S., Pathak, A., Khandaker, M. U., & Ullah, M. H. (2023). An advanced and secure framework for conducting online examination using blockchain method. Cyber Security and Applications, 1, 100005. DOI: 10.1016/j.csa.2022.100005.

[6]. "Enterprise-Grade Aml Threat Detection Using Time Frequency Signals And Spring Boot Microservices," Journal of Computational Analysis and Applications, vol. 26, no. 02, Oct. 2025, doi: 10.48047/jocaaa.2019.26.02.01.

[7].van Oosterhout / ARES community (example classic): A Secure E-Exam Management System. ARES 2006 proceedings. DOI: 10.1109/ARES.2006.14.

[8].Onyeashie, B. I., Leimich, P., McKeown, S., & Russell, G. (2025). Forensic JPEG watermarking for disk image leak attribution: An adaptive DCT–DWT approach. Electronics, 14(9), 1800. DOI: 10.3390/electronics14091800.

[9] S. R. Nelluri and P. Tatikonda, "A Comparative Study Of Aws Relational, Data Warehouse, And Nosql Databases: Advantages Over Traditional Database Systems," International Journal of Engineering Science and Advanced Technology, vol. 24, no. 1, pp. 158–165, Jan. 2024, doi: 10.64771/ijesat.2024.v24.i01.pp158-165.

[10]. "Teradata-Driven Big Data Analytics For Suspicious Activity Detection With Real-Time Tableau Dashboards," International Journal For Innovative Engineering and Management Research, vol. 5, no. 1, Oct. 2025, doi: 10.48047/ijiemr/v05/issue01/11.

[11].Sadayapillai, B. (2022). A blockchain-based framework for transparent, secure and verifiable online examination systems. Int. Journal / World Scientific. DOI: 10.1142/S1752890922410021.

[12] Sankar Das, S. (2024). Harnessing data lineage: making artificial intelligence smarter using data governance Frameworks. International Journal of Research and Analytical Reviews, 11(1). https://doi.org/10.56975/ijrar.v11i1.322571.

[13].Hylton, K., Levy, Y., & Dringus, L. P. (2016). Utilizing webcam-based proctoring to deter misconduct in online exams. Computers & Education, 92–93, 53–63. DOI: 10.1016/j.compedu.2015.10.0

Received: 10-11-2025 | Accepted: 24-12-2025 | Published: 31-12-2025 | www.ajaccm.com