IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 12, December 2025

DOI: 10.17148/IJIREEICE.2025.131210

Fingerprint Based Exam Hall Authentication System

P. Thirupathi[1], V Rahul[2], D Ganesh Reddy[3], K Narender[4], G Uday Kiran[5]

Assistant Professor, Department of Electronics & Communication Engineering,

Christu Jyothi Institute of Technology & Science, Jangaon, Telangana, India[1]

UG Student, Department of Electronics & Communication Engineering,

Christu Jyothi Institute of Technology & Science, Jangaon, Telangana, India[2-5]

Abstract: In educational institutions, ensuring the integrity of exams and preventing malpractice is a growing concern. Traditional methods of student authentication during exams, such as student ID cards or roll call, are prone to human errors and fraud. This paper proposes a fingerprint-based exam hall authentication system to improve security and ensure accurate identity verification. By leveraging biometric fingerprint recognition, the system provides a more secure, efficient, and automated solution for confirming student identity before and during exams.

The proposed system captures the student's fingerprint using a fingerprint scanner, which is then matched with a pre-enrolled fingerprint database to authenticate the student. This approach eliminates the possibility of impersonation and helps to prevent cheating. Additionally, the system records each authentication event, creating a reliable log that can be used for audit purposes.

The implementation of the fingerprint-based system not only enhances security but also streamlines the exam process by reducing the need for manual checks and enhancing the overall exam experience. Furthermore, the system can be integrated with existing exam management software to facilitate seamless operations.

I. INTRODUCTION

In the modern academic environment, maintaining fairness, transparency, and authenticity in examinations is a matter of great importance. Educational institutions across the globe continuously face challenges in ensuring that only legitimate candidates participate in exams. Conventional identity verification methods, such as manual attendance registers, photo identity cards, or hall tickets, are vulnerable to misuse, duplication, and impersonation. These traditional approaches often rely on human supervision, which is prone to error and manipulation. As a result, the overall integrity of the examination process may be compromised, leading to issues such as proxy attendance, unauthorized access, and fraudulent participation.

In order to overcome these challenges, biometric authentication has emerged as a robust and reliable solution for identity verification. Biometric systems utilize measurable physiological or behavioral characteristics—such as fingerprints, facial patterns, iris structures, or voice signatures— to uniquely identify individuals. Among these, fingerprint recognition stands out due to its universality, uniqueness, permanence, and ease of acquisition. Every individual's fingerprint possesses a distinct ridge and valley structure that remains constant throughout life, making it an ideal trait for reliable and tamper-proof identification. The advancement of fingerprint sensing technologies and pattern-matching algorithms has further enabled the deployment of such systems in real-time applications with high accuracy and efficiency.

The **Fingerprint-Based Exam Hall Authentication System** is designed to ensure that only authenticated students are granted access to the examination hall. The system operates in two main phases: **enrollment** and **authentication**. During enrollment, each student's fingerprint is scanned and stored in a secure database alongside their personal and academic details. During the authentication phase, the student places their finger on the fingerprint scanner before entering the exam hall. The captured fingerprint image is processed, and key features such as minutiae points are extracted. These features are then compared with the pre-stored template in the database using a matching algorithm. A successful match confirms the identity of the student, thereby granting access, while a mismatch denies entry.

This automated authentication process eliminates the possibility of proxy attendance and manual errors, ensuring that only the rightful candidates appear for the examination. Furthermore, it significantly reduces administrative workload by automating attendance management and identity verification. The system enhances operational efficiency by

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 12, December 2025

DOI: 10.17148/IJIREEICE.2025.131210

providing fast, accurate, and contact-based verification without the need for physical ID cards or manual records. Additionally, the digital nature of data storage and verification facilitates easy integration with other institutional systems such as student databases, attendance records, and exam management software.

By incorporating biometric technology into academic examination systems, institutions can achieve a higher level of security, accountability, and transparency. The proposed fingerprint-based authentication model not only addresses the limitations of traditional methods but also aligns with modern trends in digital identity management and smart campus solutions. The system's adaptability and scalability make it suitable for universities, colleges, and even competitive examination centers. Ultimately, this approach promotes a secure, efficient, and technology- driven examination environment that upholds academic integrity and minimizes the risk of malpractice.

II. PROPOSED SYSTEM

The proposed **Fingerprint-Based Exam Hall Authentication System** aims to enhance the **security, efficiency, and integrity** of the examination process by integrating **biometric fingerprint recognition** with additional authentication mechanisms. The system is designed to verify the identity of students before allowing entry into the examination hall, ensuring that only authorized individuals participate. By leveraging biometric technologies, the proposed model eliminates traditional vulnerabilities such as impersonation, misuse of hall tickets, and manual verification errors.

To further strengthen the verification process, the system employs a **Multi-Factor Authentication (MFA)** approach that combines two or more independent credentials, thus providing layered security.

- **Fingerprint + Facial Recognition:** Students are required to successfully pass both fingerprint and facial recognition scans before being granted access. This dual verification mechanism ensures that even if one biometric modality is compromised, the other serves as an additional safeguard.
- **Smart Card + PIN Verification:** For added flexibility, the system allows the use of a registered smart card combined with a personal identification number (PIN). This hybrid model ensures secure access control, especially in scenarios where biometric devices face technical constraints.
  The proposed system also integrates **contactless biometric technologies** to improve hygiene, convenience, and accessibility.
- **3D Facial Recognition:** Utilizes advanced imaging sensors to capture a detailed three- dimensional representation of the student's face, allowing authentication without any physical contact with the device.
- **Iris Scanning:** Performs high-precision scanning of the iris from a distance, ensuring quick and hygienic verification. This feature is particularly beneficial in large-scale examination setups where multiple students are verified simultaneously.

III. LITERATURE REVIEW

Biometric solutions—especially fingerprint recognition—are widely proposed to secure examination halls and automate attendance because of their distinctiveness, permanence, and relatively low cost. Several project-level implementations and short papers demonstrate feasibility using microcontrollers (Arduino/Raspberry Pi), off-the-shelf fingerprint modules, and local databases; these works report acceptable accuracy in controlled settings but note practical issues such as enrollment quality, sensor hygiene, and template management.

A. Project / Prototype implementations

1. Vaishnavi Kulkarni, Mangita Waghmare, Supriya Gund, D. B. Shivpuje (2019). "Fingerprint Based Exam Hall Authentication" — a practical implementation integrating a fingerprint sensor with a microcontroller and local storage to allow/deny exam entry. The authors describe enrollment and verification modes and report prototype- level performance suitable for small deployments.

2. K. Subbalakshmi, M. Bhagavathi, S. Surendhar et al. (IJEET, 2021). "Exam Hall Authentication Using Finger Print" — presents an Arduino-based system that stores multiple user templates and verifies candidates at the gate. The paper discusses response time and basic false accept/reject observations in small trials.

3. Various conference and open access reports (IRJET, IJRASET, IJARSCT, 2017–2025).

Multiple groups publish similar designs: fingerprint module (R305/R307/R503),microcontroller/Arduino or Raspberry Pi, and simple SQL/CSV storage for templates and attendance logging; several works add IoT features to upload logs to a central server. These reports consistently show that low-cost fingerprint modules can enable practical exam-level authentication with short scan times (~1–3 s) in low to moderate throughput scenarios.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 12, December 2025

DOI: 10.17148/IJIREEICE.2025.131210

IV. EMBEDDED SYSTEMS

An embedded system is a specialized computing system designed to perform dedicated functions or tasks within a larger system. Unlike general-purpose computers, embedded systems are optimized for specific applications and often have constraints in terms of processing power, memory, and storage. They are typically integrated with hardware and run software (often called firmware) that directly interacts with that hardware.

Embedded systems are used in a wide range of applications, from household appliances like washing machines and microwaves to critical systems in automobiles, healthcare devices, industrial machines, and consumer electronics. These systems are designed to be reliable, efficient, and real-time, often operating continuously with minimal human intervention.

Embedded systems are integral parts of modern life, from controlling household appliances to ensuring safety in automobiles. These systems are usually designed with a focus on efficiency, reliability, and specific functionality. As technology evolves, the role of embedded systems is growing, especially in the realm of the Internet of Things (IoT), where many devices are becoming interconnected and smarter.

V. ANALYSIS AND DESING

The **fingerprint-based exam hall authentication system** operates using biometric fingerprint recognition to verify the identity of students entering an exam hall. Below is a step-by-step breakdown of how the system works.

1. **Student Enrolment**
   - **Fingerprint Capture:** When a student registers for the exam, their fingerprint is captured using a **fingerprint scanner**. This scanner captures the unique ridges and patterns in the student's fingerprint.
   - **Data Processing:** The fingerprint data is processed and converted into a digital template (a mathematical representation of the fingerprint). This template, which is unique to the individual, is then stored in a secure database along with the student's other details (e.g., name, student ID, course).
   - **Secure Storage:** The fingerprint data is encrypted to protect student privacy and ensure security. Only authorized personnel have access to this data.

2. **Entry to Exam Hall**
   - **Fingerprint Scanning at Entry:** On the day of the exam, as the student arrives at the exam hall, they are directed to a **fingerprint scanner** placed at the entrance.
   - **Fingerprint Enrolment Check:** The student places their finger on the fingerprint scanner. The scanner reads the fingerprint and converts it into a digital template for comparison.

3. **Verification Process**
   - **Matching with Stored Template:** The system compares the scanned fingerprint with the template stored in the database. The comparison looks for **minutiae points** (unique features like ridge endings, bifurcations, etc.) to find an exact match.

   - **Authentication Decision:**
     - **Match Found:** If the fingerprint matches a record in the database, the system confirms the student's identity, grants access, and logs the time of entry.
     - **No Match:** If the fingerprint does not match any record, the student is either denied entry or prompted for assistance (e.g., a manual check can be done by staff if there's an issue).

System Flow Summary:

i. **Enrolment:** Capture and store fingerprint data of the student.
ii. **Entry Verification:** Scan the student's fingerprint upon arrival at the exam hall.
iii. **Matching:** The scanned fingerprint is compared with the stored database.
iv. **Authentication:** If the fingerprint matches, the student is granted access and logged. If not, further verification occurs.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 12, December 2025

DOI: 10.17148/IJIREEICE.2025.131210

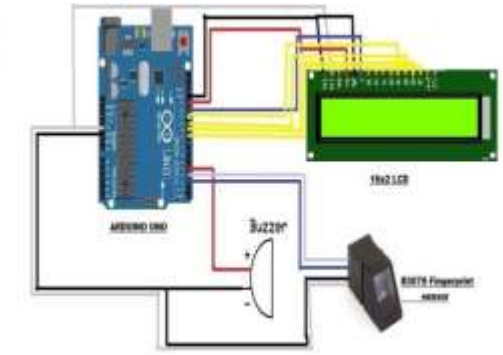

Fig. Circuit Finger print Based Exam Hall Authentication System.

VI. SOFTWARE USED

Arduino is a prototype platform based on an easy-to-use hardware and software. It consists of a circuit board, which can be programmed and a ready-made software called Arduino IDE, which issued to write and upload the computer code to the physical board. **Key Features:**

- Arduino boards are able to read analog or digital input signals from different Sensors and turn it into an output such as activating a motor, turning LEDon/off, connect to the cloud and many other actions.
- It can control the board functions by sending a set of instructions to the microcontroller on the board via Arduino IDE.
- Most previous programmable circuit boards, Arduino does not need an extra piece of hardware (called a programmer) in order to load a new code onto the board. You can simply use a USB cable.
- Additionally, the Arduino IDE uses a simplified version of C++, making it easier to learn to program.
- Finally, Arduino provides a standard form factor that breaks the functions of the microcontroller into a more accessible package. After learning about the main parts of the Arduino UNO board, we are ready to learn how to set up the Arduino IDE. Once we learn this, we will be ready to upload our program on the Arduino board.

Figure: Arduino IDE

VII. RESULT

Successful authentication:

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 12, December 2025

DOI: 10.17148/IJIREEICE.2025.131210

Failed Authentication:

VIII. CONCLUSION

In conclusion, fingerprint-based exam hall authentication offers a promising solution to enhance the security and integrity of examination processes. By leveraging the unique nature of fingerprints, this method can significantly reduce instances of impersonation and ensure that only authorized candidates participate. The speed and accuracy of fingerprint scanning make the process more efficient compared to traditional verification methods, improving overall exam management. However, challenges such as potential false matches, privacy concerns, and the costs of implementation must be addressed to ensure its effectiveness. Despite these hurdles, fingerprint authentication stands as a valuable tool for maintaining fairness and security in exams, making it a viable option for modern educational institutions.

IX. FUTURE SCOPE

The future scope of fingerprint-based exam hall authentication includes the following potential developments:

1. **Integration with Other Biometric Systems**: Combining fingerprint authentication with other biometric methods like facial recognition or iris scanning for enhanced security and accuracy.
2. **Cloud-Based Systems and Data Security**: Secure storage and processing of biometric data on cloud platforms, enabling centralized monitoring and real- time analytics of exam security across multiple locations.
3. **Automated Monitoring and AI Integration**: Integration of artificial intelligence to detect suspicious behaviors, anomalies, or discrepancies in real- time, adding an extra layer of security during exams.
4. **Increased Accessibility and Affordability**: As biometric technology becomes more affordable, fingerprint authentication could be adopted by institutions globally, including those in developing regions, enhancing accessibility.

REFERENCES

Fingerprint Authentication Basics

[1]. **"Handbook of Fingerprint Recognition"** by Maltoni et al.
Covers fingerprint recognition principles and techniques.

[2]. **"Introduction to Biometrics"** by Jain et al.
A great starting point for understanding biometric systems, including fingerprints.

Fingerprint Matching Algorithms

[1]. **"Fingerprint Matching Using a Hybrid Scheme"** by Lee and Hsu.
Discusses fingerprint matching techniques for enhanced security.

Biometric Authentication for Exams

[1]. **"Biometric Authentication in e- Exams: A Review"** by Ekinci and Kose.
Focuses on using biometric systems (like fingerprints) to secure exams.

Practical Systems

[1]. **Neurotechnology Veri Finger SDK** and **MorphoSmart SDK**.
Software tools to implement fingerprint recognition in your project.