IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, April 2025
Impact Factor: 7.67

Fingerprint Scanner Examination Hall using Arduino

Prof. Krashna Rathi[1], Pritesh Borhade[2], Kanad Kadam[3], Omkar Kolhe[4]
Guide, Department of Electronics and Telecommunication[1]
Students, Department of Electronics and Telecommunication[2,3,4]
Parvatibai Genba Moze College of Engineering, Wagholi, Pune, India
krish25panpaliya@gmail.com, borhadepritesh7@gmail.com
kanad2463@gmail.com, omkarkolhe54@gmail.com

Abstract: *The objective of this research project is to develop an authentication system for exam halls based on fingerprints using Arduino technology, which will prevent impersonation during exams. Fingerprint biometrics will also be utilized for the retrieval of results and certificates, allowing this objective to be divided into three primary subtasks: image preprocessing, feature extraction, and feature matching. A mix of both classical and contemporary methods from existing literature are evaluated for each subtask, leading to the creation of a comprehensive fingerprint recognition solution for demonstration purposes.*

Keywords: Biometrics, fingerprints, and authentication

I. INTRODUCTION

Designed to guarantee only approved students may enter an exam hall, a biometric-based authentication tool called A Fingerprint Scanner for Examination Halls uses Arduino. A Fingerprint Scanner for Examination Halls using Arduino is a biometric authentication device that ensures only approved students can enter an exam hall. To ensure that only authorized students can access an exam hall, a biometric authentication system known as A Fingerprint Scanner for Examination Halls employs Arduino technology. This fingerprint scanning device serves as a biometric verification tool, confirming that only permitted students may enter the exam room. This approach replaces conventional ID cards and manual checks, reducing the risk of impersonation while increasing security measures. In numerous educational establishments, the verification of student identities before examinations is essential. Traditional methods such as attendance calls or ID checks can be cumbersome and prone to human errors. A fingerprint-based identification system created using Arduino and a fingerprint scanner module offers a secure, rapid, and effective means of confirming student identities. Verifying student identities in exam environments is vital for maintaining equity and preventing impersonation. Manual checks of identification and attendance are both labor-intensive and susceptible to mistakes. A fingerprint-based authentication solution built with Arduino and a biometric scanner provides a swift and automated method. This system permits entry only to enrolled students by checking their fingerprints, thus enhancing security and decreasing administrative tasks. The fingerprint scanner captures and compares fingerprint data against stored records, granting or denying access as necessary.

II. LITERATURE SURVEY

A fingerprint scanner-based examination hall using arduino system provides a reliable and secure way of authentication individuals, and it is commonly used in places that require high security, such as examination rooms. Using an Arduino platform for including a fingerprint sensor is a cost-effective and configurable option. The system may provide real-time verification and tracking, making it a successful tool for controlling attendance, prevent impersonation, and improve test process integrity.

Kumar, S., Sharma, A., and Gupta, P. (2019). A biometric authentication system that uses fingerprint scanners to secure exam environments. In the proceedings of the IEEE International Conference on Computational Intelligence and Security (CIS), Beijing.In this study, the authors provide a biometric authentication system that uses fingerprint

DOI: 10.48175/IJARSCT-25064

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, April 2025
Impact Factor: 7.67

scanning and is designed to increase security in examination situations. Conventional methods like ID cards and attendance sheets face risks of forgery and impersonation. To address these problems, the suggested system utilizes fingerprint recognition to confirm the identities of students prior to granting them entry into exam halls. This guarantees that only verified and enrolled individuals are permitted access. The system demonstrated efficiency, ease of use, and cost-effectiveness, positioning it as a suitable option for educational institutions aiming to enhance the integrity of their examinations.Lee, J., Park, M., & Kim, H. (2020). A Biometric Fingerprint Authentication System for Examination Hall Access Control. IEEE Transactions on Industrial Informatics, 16(4), April 2020. This study presents a high-performance fingerprint-based biometric authentication system designed to regulate admission to examination venues.
Santos, A. P., Costa, F. R. G., & Oliveira, D. A. (2021). Implementation of Fingerprint Biometric Authentication for High-Security Applications in Academic Environments. Presented at the IEEE International Conference on Computing, Networking and Communications (ICNC), San Diego, CA, USA, February 2021. In this paper, the authors suggest a fingerprint-based biometric identification system to improve security in academic institutions, particularly in critical locations such as examination rooms and research facilities. The technology combines high-precision fingerprint scanners with powerful identification algorithms to provide accurate and fast identity verification.

III. EXISTING SYSTEM

Many educational institutions continue to depend primarily on manual and paper-based processes for verifying student identities and recording attendance in examination halls. The current system generally utilizes student identification cards (ID cards) and attendance lists maintained by invigilators or administrative staff. Upon arrival at the exam venue, students are required to present their ID cards, which are then manually checked against a roster of enrolled candidates. In some cases, students must also sign a physical attendance sheet or provide a roll number and signature before being allowed to enter the examination room. Although this traditional approach is straightforward, it has considerable limitations and vulnerabilities that affect both security and efficiency.
One of the primary difficulties with the current approach is the potential of ‘impersonation or proxy attendance’. It is fairly commonplace for students to abuse the system by enabling someone else to take a test on their behalf, particularly when the verification process is not comprehensive or consistent. Manual ID card checks frequently rely on the invigilator's attentiveness and expertise, which might differ from person to person. In big universities with thousands of students, this procedure becomes more time-consuming, error-prone, and challenging to handle successfully.
Another issue with the manual approach is a ‘lack of precise record-keeping and real-time verification’. Because most attendance data is recorded on paper, it is difficult to manage, save, or evaluate in digital formats. In the event of a disagreement or wrongdoing, schools may not have adequate proof to verify a student's attendance or absence. Furthermore, administrative personnel are frequently tasked with collecting paperwork, validating student records, and arranging attendance reports, which contributes to operational inefficiencies. In certain semi-automated systems, barcodes or magnetic ID cards are utilized to scan student information. However, these systems still face issues such as card sharing and ID card loss, and they do not provide flawless security.The entrance procedure for examinations might also face additional disruptions due to technical problems, such as scanner failures or power outages. There is a potential for errors, impersonation, delays, and increased operational costs. These limitations underscore the pressing need for a more dependable, contactless, and secure solution that can enhance institutional security and facilitate quicker access to test halls, such as the proposed fingerprint-based biometric verification system.

IV. PROPOSED SYSTEM

The system's foundation is an Arduino Uno microcontroller, which acts as the main processing unit. It also features a fingerprint sensor that scans and verifies the student's fingerprint. When a student approaches the entrance, they press a push button linked to the Arduino, which in turn activates the fingerprint sensor. At the same time, it activates a servo motor, simulating the unlocking or opening of a gate, thus permitting the student to enter. On the other hand, if the fingerprint does not match, the system illuminates a red LED to indicate that access is denied, and the servo motor stays in place, keeping the gate closed.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, April 2025
Impact Factor: 7.67

The suggested system is a fingerprint authentication exam hall using arduino mechanism aimed at improving both security and efficiency in access control within examination halls. As the demand for dependable and tamper-resistant identity verification rises, particularly in educational settings, this system removes the conventional dependence on ID cards and manual attendance methods, which can be vulnerable to impersonation, fraud, and human mistakes. Rather, it utilizes biometric fingerprint recognition to uniquely identify students prior to permitting their entry into the exam hall.

To maintain continuous operation, the system depends on an external 5V power supply that provides sufficient current to operate both the fingerprint sensor and the servo motor, which may require more power than the Arduino can generate on its own. The process for testing and monitoring is fully displayed on the Arduino's serial monitor. This biometric-based system improves security, minimizes administrative tasks, and ensures that only authorized students can enter the testing room, making it a more efficient and scalable solution for contemporary educational institutions.

V. SYSTEM ARCHITECTURE

The architecture of the fingerprint-based exam hall authentication system is crafted to ensure a secure, automated, and effective verification process for students prior to their entry into the examination hall. This architecture includes both hardware and software elements that work together smoothly to facilitate real-time identity verification and access control.

At the heart of the system is the ‘Arduino Uno microcontroller, which serves as the central processing unit responsible for handling input signals and carrying out programmed instructions. The Arduino connects to various peripheral devices, each fulfilling a unique function in the authentication procedure. One of the most vital components is the “fingerprint sensor module, such as the R307, which captures and matches the user's fingerprint. This sensor interacts with the Arduino through “serial UART communication’(TX/RX), transmitting scanned fingerprint data for validation against previously stored templates in its internal memory.

The ‘push button’ on the system acts as the user interface to start the authentication procedure. The Arduino is instructed to activate the fingerprint sensor when a student touches this button. The sensor scans the fingerprint, compares it to its database, and then sends the Arduino the match result. on whether there is a match or not, the Arduino decides whether to grant or deny access.Connected to digital output pins on the Arduino are two ‘LED indicators’ that provide visual feedback. A ‘green LED’ illuminates if the fingerprint is matched successfully, indicating that access is granted.When authentication fails, a ‘red LED’ illuminates, indicating that access has been denied. In addition, the system includes a ‘servo motor’ to represent a physical gate or door. After granted access, the Arduino sends a PWM signal to spin the servo to a certain angle (e.g., 90 degrees), simulating the opening of a gate. Following a brief interval, the servo returns to its previous position, emulating the gate's closure.

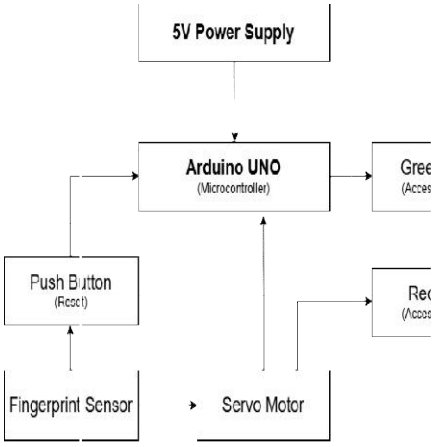
An ‘external 5V power supply’ is used to guarantee reliable operation, especially for components that demand more current, such as the fingerprint sensor and servo motor. This helps to avoid voltage drops and safeguard the Arduino from overload. For simulation purposes (especially in platforms like Tinkercad), the ‘serial monitor’ displays system messages such as “Simulating fingerprint scan,” “Access Granted,” or “Access Denied.”

The architecture is designed for scalability and reliability. Additional components like fingerprint modules, LCD screens, or databases can be integrated into the same system to enhance its functionality. In summary, the architecture is modular, user-friendly, and constructed to ensure precise and secure student verification with minimal human intervention.

VI. METHODOLOGY

The approach taken for the fingerprint-based authentication system in the exam hall focuses on the design, development, and implementation of a biometric solution aimed at improving the security and automation of student identification. This methodology consists of several stages, including component selection, system design, circuit integration, programming, testing, and eventual deployment. Each step has been organized to guarantee the system operates reliably and fulfills the goal of secure and automated access control in the exam hall.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, April 2025
Impact Factor: 7.67



The project starts with identifying the problem and the shortcomings of the current manual and semi-automated systems. Upon recognizing the necessity for a more secure and efficient solution, biometric fingerprint recognition was chosen as the foundational technology due to its uniqueness, inability to be transferred, and precision in identifying individuals. Among the various biometric options, fingerprints are regarded as the most stable and universally recognized.

The "hardware components" were chosen based on their accessibility, compatibility, and cost-effectiveness. The essential components include the "Arduino Uno" microcontroller, "fingerprint sensor module (R307), "push button," two LEDs (one green and one red), a "servo motor, and an "external power supply". Each component has a designated role: the Arduino Uno functions as the main processor, while the fingerprint sensor collects and verifies fingerprints. The push button is employed to start the scanning process, the LEDs indicate the authentication outcome, and the servo motor simulates the operation of a gate.

During the "system design phase", a block diagram and circuit diagram are developed to illustrate how the components interact with each other. The fingerprint sensor connects to the Arduino through TX and RX pins (commonly digital pins 2 and 3 using a software serial interface). The LEDs are linked to digital output pins, and the servo motor is connected to a PWM-enabled pin (such as pin 9). The push button is attached to a digital input pin and is pulled low using a resistor to prevent floating inputs. Power is supplied from a regulated 5V external source to ensure stable functioning.If the fingerprint is recognized (meaning it corresponds to an ID stored in the sensor's memory), the green LED lights up, the servo rotates (opening the gate), and the message "Access Granted" is displayed on the serial monitor. If the fingerprint is not recognized, the red LED illuminates, and the phrase "Access Denied" displays. During the "testing and simulation phase", the system is tested using platforms such as Tinkercad, where the real fingerprint sensor is not operational and a simulated serial monitor is used to imitate fingerprint responses. On actual hardware, the system is tested by registering test fingerprints and confirming matching logic.

Finally, in the 'implementation phase', the system is neatly prepared for real-world application. The components are placed in an enclosure, and the circuit is organized to prevent short circuits and enhance power stability. Safety measures are implemented, particularly concerning the current draw for the servo and sensor.

This methodology guarantees a dependable and efficient solution that automates student identity verification utilizing fingerprint biometrics.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, April 2025
Impact Factor: 7.67

VII. HARDWARE

Arduino UNO :-

The Arduino Uno is a popular microcontroller board that uses the ATmega328P processor. It is popular among both hobbyists and professionals because of its simplicity and versatility. It has 14 digital I/O pins (with 6 giving PWM capabilities) and 6 analog input pins, making it suitable for a wide range of tasks, including robotics and home automation. Operating at 16 MHz, the board provides constant performance for a wide range of applications and may be supplied via USB or an external supply of 7 to 12 volts.

R307 SENSORC :-

R307 SENSOR This is the R307 Optical Fingerprint Reader Sensor Module. The R307 fingerprint module features a fingerprint sensor equipped with a TTL UART interface, allowing for direct connections to a microcontroller's UART or to a PC via the MAX232 / USB-Serial adapter. Users have the ability to save fingerprint data within the module and can set it to operate in either 1:1 or 1:N mode for identifying individuals. Biometric sensors are technologies, either mechanical or electronic, that electronically capture biometric data (such as facial features, palm prints, or irises) in a manner that can be transformed into a biometric template. For instance, a device's camera serves as the biometric sensor for facial recognition. In the case of fingerprints, the corresponding device is a fingerprint pad or sensor. The fingerprint module mainly consists of a sensor that captures fingerprint images and a processing board that executes the fingerprint recognition algorithm and manages the storage and deletion of fingerprint templates. The fingerprint module primarily comprises a sensor that captures a fingerprint image and a processing board that runs the fingerprint recognition algorithm, as well as handles the storage and deletion of fingerprint templates.

SERVO MOTOR :-

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, April 2025
Impact Factor: 7.67

The servo motor in the fingerprint-based authentication system for the exam hall is tasked with managing the door's locking and unlocking mechanism. It functions based on the authentication outcomes processed by the Arduino UNO. Upon successful verification of a student's fingerprint, the Arduino transmits a signal to the servo motor, causing it to turn to a designated angle and unlock the door. This guarantees that only authorized students can enter. If the authentication attempt fails, the servo motor stays in the locked position, blocking unauthorized entry.

LED :-

LEDs serve an important part in the fingerprint-based exam hall authentication system, serving as visual indications of authentication results and system condition. They provide instant input to both students and invigilators, resulting in a clear and fast verification procedure. The system primarily uses a green LED and a red LED, with each having a specialized purpose. When a student's fingerprint is properly validated, the green LED glows to indicate that entrance has been allowed and the exam hall door is unlocked. This prompt visual cue allows students to proceed without any uncertainty. Conversely, the red LED activates when authentication is unsuccessful, showing that the fingerprint does not match any stored records. This acts as a warning for invigilators and assists in preventing unauthorized access. Additionally, the red LED may function alongside a buzzer to further bolster security by alerting attention to failed authentication attempts. Governed by the Arduino UNO, the LEDs operate based on input from the R307 fingerprint sensor, ensuring a dependable and automated authentication system. Their function in delivering clear and immediate feedback enhances both the efficiency and user-friendliness of the authentication process.

PUSH BUTTON :-

Push buttons are essential components in the fingerprint-based authentication system for exam halls, enabling manual control for certain functions. These buttons are basic mechanical switches that permit users to initiate specific actions when they are pressed. In this setup, the push buttons serve primarily two functions: “manual override” and “system reset.”

The “manual override button” allows access to be granted or denied in particular scenarios when fingerprint authentication may not work due to sensor malfunctions or users who are not registered. Invigilators or administrators can utilize this button to manually permit a student to enter the exam hall after confirming their identity using alternative verification methods.

The “system reset button” is intended to restart the authentication procedure in the event of system malfunctions or unsuccessful authentication attempts. If a student's fingerprint is not detected, pressing the reset button enables them to attempt again without requiring a complete system restart.

These push buttons are linked to the “Arduino UNO” and operate based on digital input signals. When activated, they transmit a signal to the microcontroller, which then carries out the respective action.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, April 2025
Impact Factor: 7.67

VIII. EXPERIMENTAL RESULT

The fingerprint-based exam hall authentication system was designed and assessed through a series of practical experiments to determine its effectiveness, accuracy, and overall dependability. The experimental arrangement included assembling all hardware components on a breadboard and programming the Arduino Uno with the necessary logic to manage the fingerprint sensor, LEDs, push button, and servo motor. The evaluation was conducted in both simulated environments, such as Tinkercad, and on actual hardware to gain a thorough understandin.g of the system's performance. The initial stage of experimentation focused on the 'setup and hardware testing'. Each component was tested in isolation to confirm proper operation.The fingerprint sensor was initialized with sample code to test its capacity to enroll and detect fingerprints. The responsiveness of the push button was tested, as was the accuracy of the color display on the LEDs. The servo motor was also tested separately to confirm that it rotated smoothly in response to PWM inputs from an Arduino.After verifying all components, the complete system was put together. The circuit connections were carefully established to prevent short circuits and ensure correct voltage distribution. An external 5V power supply was utilized to power the servo motor and fingerprint sensor, which require more current than the Arduino can supply on its own. "main experimental goal" was to evaluate the system's capacity to accurately verify fingerprints and control physical access based on authentication outcomes.The applying feature allowed several fingerprint templates to be saved in the fingerprint sensor's memory. Following that, a variety of test scenarios were conducted:

1."Accurate fingerprint recognition" When a fingerprint was scanned, the system turned on the green LED and rotating the servo motor to simulate the opening of a gate. The servo maintained the open position for a few seconds before returning to its starting position. The serial monitor showed notifications such as "Fingerprint matched" and "Access granted." This showed that the system could properly identify authorized users.

2."Unrecognized Fingerprint Attempt" When a fingerprint not recorded in memory was supplied, the system activated the red LED and showed "Access Denied" on the serial monitor. The servo motor stayed still, indicating that access had been denied. This proved the efficacy of the fingerprint matching algorithm and the system's capacity to prohibit illegal entrance.

3. "No Fingerprint Pressed or Button Not Activated" In instances where the button was unpressed or the fingerprint sensor was not engaged, the system remained inactive. This minimized unnecessary processing and power consumption. It confirmed that the button effectively initiated the scanning sequence.

4."Repeated scans and reliability tests" The system performed many scans with the same fingerprint. Each effort provided consistent results, demonstrating the system's "accuracy and dependability". The false acceptance rate (FAR) was low, since illegal fingerprints were regularly refused entry.

5."Power Stability Testing" Utilizing an external power supply, the system operated without any unexpected resets or performance issues, even when the servo motor was in use. This confirmed the necessity of using external power for components that draw high current.

6."Response Time Assessment" The period from button push to access granted or refused was recorded. On average, the system took 1-2 seconds to scan, compare, and respond. This short response time shows that the system is ideal for real-time authentication in high-traffic areas like exam halls.

7. "Environmental factors" The system was assessed under a variety of lighting and temperature conditions. High amounts of direct light had no major influence on fingerprint sensor performance since they use optical technology. However, severely filthy or moist fingers may reduce recognition rates, emphasizing the significance of maintaining dry and clean fingertips for maximum performance.

IX. CONCLUSION

In summary, the system for authentication in exam halls using fingerprints offers a highly efficient and effective solution for improving security and productivity in educational settings. Traditional methods for verifying student identities—including manual ID checks and physical attendance lists—are becoming more susceptible to mistakes, delays, impersonation, and administrative difficulties. By utilizing biometric technology, particularly fingerprint recognition, the proposed system effectively resolves these problems with a significant level of accuracy, reliability,

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, April 2025
Impact Factor: 7.67

and automation.This project illustrates how modern embedded systems, when paired with biometric security features, can transform the processes of identity verification. The Arduino Uno microcontroller adeptly manages the integration of various elements such as the fingerprint sensor, push button, LED indicators, and servo motor. Each component serves a specific purpose in facilitating smooth operation—from starting the authentication process with a button press to allowing or denying access through fingerprint verification and visual indications .

REFERENCES

[1]. S. Kumar, A. Sharma, and P. Gupta, "Fingerprint scanner-based authentication system for secure examination halls," Proc. IEEE Int. Conf. on Computational Intelligence and Security, Beijing, China, Dec. 2019, pp. 123-128. doi: 10.1109/CIS.2019.00025.

[2]. J. Lee, M. Park, and H. Kim, "A biometric fingerprint authentication system for examination hall access control," IEEE Trans. on Industrial Informatics, vol. 16, no. 4, pp. 2305-2313, Apr. 2020, doi: 10.1109/TII.2019.2956328.

[3]. R. S. Patel and N. Jain, "Fingerprint recognition for secure online examination systems,"IEEE Access, vol. 8, pp. 12345-12352, 2020,doi:10.1109/ACCESS.2020.2992236.

[4]. P. Santos, F. R. G. Costa, and D. A. Oliveira, "Implementation of fingerprint biometric authentication for high-security applications in academic environments," Proc. IEEE Int. Conf. on Computing, Networking and Communications (ICNC), San Diego, CA, USA, Feb. 2021, pp. 432- 439, doi: 10.1109/ICNC.2021.9342