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 6, Issue 6, March 2026

Impact Factor: 8.2

Finger Print Based Exam Hall Authentication System

Prof. H. K. Bhangale[1], Navghare Swati Sanjay[2], Baraskar Sujit Balasaheb[3], Borge Akanksha Sandip[4], Kandekar Vaibhav Rajendra[5]

[1]Assistant Professor, Department of Electronics & Telecommunication Engineering
[2, 3, 4, 5] Students, Department of Electronics & Telecommunication Engineering
Adsul Technical Campus, Chas, Ahilyanagar.

Abstract: *Ensuring proper identification of students during examinations is essential for maintaining fairness and preventing academic malpractice. Traditional verification methods such as manual attendance and ID card checking are often slow and may allow impersonation or proxy attendance. To overcome these limitations, this study proposes a Finger Print Based Exam Hall Authentication System that uses biometric technology to accurately verify student identity before they enter the examination hall.*

The proposed system is built using a fingerprint sensor integrated with an ESP32 microcontroller, which acts as the central processing unit of the system. During the registration phase, the fingerprints of students are captured and stored securely in the system database. When a student arrives for an examination, the fingerprint sensor scans the fingerprint and sends the data to the microcontroller for comparison with stored records. If the fingerprint matches the registered data, the system grants access and records attendance automatically. In case of a mismatch, the system denies entry and triggers an alert using a buzzer. A 16×2 LCD display is used to show authentication messages such as verification status and access results.

This system improves the reliability and speed of student verification while reducing the chances of examination fraud. It also minimizes manual effort by automating the attendance process and maintaining accurate records. The proposed solution can be effectively implemented in educational institutions to enhance security and streamline examination management. Additionally, the system can be extended in the future by integrating cloud storage, real-time monitoring, and other biometric technologies to further improve efficiency and scalability.

Keywords*:* Fingerprint Authentication, Biometric Security, ESP32 Microcontroller, Exam Hall Monitoring, Student Verification System, Automated Attendance System

I. INTRODUCTION

Maintaining transparency and fairness during examinations is an important responsibility for educational institutions. One of the major challenges faced by universities and colleges is verifying the identity of students who appear for examinations. Traditional authentication methods such as manual attendance, hall ticket verification, and identity card checking are commonly used, but these methods are often slow and vulnerable to errors or misuse. In some cases, impersonation or proxy attendance may occur, which can affect the credibility of the examination system and reduce trust in academic evaluation processes [1].

With the advancement of technology, biometric authentication systems have emerged as a reliable solution for identity verification. Biometric systems use unique biological characteristics such as fingerprints, facial features, iris patterns, or voice recognition to identify individuals. Among these methods, fingerprint recognition is widely accepted due to its accuracy, uniqueness, cost-effectiveness, and ease of implementation in real-world applications [2]. Fingerprints are

DOI: 10.48175/568

unique for every individual, and even identical twins do not share the same fingerprint patterns, making it a highly secure method for authentication [3].

In recent years, fingerprint-based systems have been increasingly used in areas such as access control, employee attendance management, banking security, and mobile device authentication. These systems help in reducing manual work while improving the speed and accuracy of identification processes [4]. In the context of educational institutions, integrating biometric technology into examination management systems can significantly reduce the chances of impersonation and improve the efficiency of student verification [5].

The Finger Print Based Exam Hall Authentication System is designed to automate the process of verifying students before they enter the examination hall. In this system, students are required to register their fingerprints in advance, which are stored securely in a database. During the examination, the fingerprint sensor scans the student's fingerprint and compares it with the stored template to confirm their identity. If the fingerprint matches the registered data, the system grants access and records the attendance automatically [6].

The system uses an ESP32 microcontroller as the central processing unit to handle fingerprint processing and data verification. The ESP32 is widely used in embedded systems because of its high processing capability, wireless communication features, and low power consumption. It allows the system to operate efficiently and manage authentication processes quickly [7]. Additionally, a 16×2 LCD display is used to show system messages, and a buzzer is included to provide alerts when unauthorized access attempts are detected.

Implementing such a system in examination halls can significantly improve security and reduce the workload of invigilators. Instead of manually checking each student's identity, the system automatically verifies the student in a few seconds. This not only saves time but also ensures that the attendance records are accurate and stored digitally for future reference [8].

Another advantage of fingerprint-based authentication systems is their scalability. The system can be expanded to support large numbers of students and can be integrated with institutional databases or cloud-based systems for centralized management. This makes the solution suitable for universities, colleges, and large examination centers where efficient identity verification is required [9].

Furthermore, the adoption of biometric authentication in educational environments supports the development of smart campus infrastructure. It enables institutions to integrate security systems with digital attendance, access control, and examination management platforms, creating a more reliable and automated system [10].

II. PROBLEM STATEMENT

In many educational institutions, the process of verifying students during examinations is still carried out using traditional methods such as checking identity cards, hall tickets, or maintaining manual attendance registers. While these methods are simple, they often create several challenges related to security, efficiency, and accuracy. Manual verification requires invigilators to check each student individually, which becomes time-consuming and difficult when a large number of students are present for an examination. This can lead to delays at the entrance of exam halls and increases the workload of staff members responsible for monitoring the examination process. Another major issue with traditional systems is the risk of impersonation or proxy attendance, where an unauthorized person may attempt to write an exam on behalf of a registered student by using borrowed or fake identification. Since manual checking mainly depends on visual verification, it is not always possible to detect such fraudulent activities effectively. In addition, maintaining attendance through paper-based registers can lead to human errors such as incorrect entries, missing records, or duplication of data, which makes it difficult to manage and track attendance accurately over time. Security concerns also arise because traditional systems do not provide a reliable mechanism to ensure that only authorized students are allowed to enter the examination hall. Moreover, the lack of automation means that real-time verification and digital record management are not available, which reduces the overall efficiency of the examination process. Therefore, there is a strong need for a secure, fast, and automated authentication system that can accurately verify student identities and prevent unauthorized access. A fingerprint- based biometric system offers a reliable solution to these problems because fingerprints are unique to each individual and cannot be easily duplicated, making the examination process more secure, efficient, and trustworthy.

III. OBJECTIVE

- To develop a fingerprint-based authentication system for verifying student identity before entering the examination hall.
- To prevent impersonation and unauthorized entry during examinations by using biometric verification.
- To automate the attendance process and reduce manual effort for invigilators and exam authorities.
- To improve the security and reliability of the examination management system.
- To ensure fast and accurate identification of students using a fingerprint sensor integrated with a microcontroller system.

IV. LITERATURE SURVEY

Paper Name: Development of a Fingerprint-Based Attendance Monitoring System
Year: 2025
Publication / Journal: ABUAD Journal of Engineering Research and Development (AJERD)
Authors: Gerard Obiora, Isreal Oluwaseun Aladejare, Godwin Osariemen Igbinosa, Collins Belouebi Fiemobebefa
Summary: This research focuses on the design and implementation of a fingerprint-based attendance monitoring system aimed at improving the efficiency of attendance management in educational institutions. The authors highlight that traditional attendance systems often rely on manual recording methods, which can lead to errors, manipulation, and difficulty in maintaining records over long periods. The proposed system uses biometric fingerprint authentication to ensure that each student's identity is verified accurately before attendance is recorded. The study demonstrates that integrating biometric technology significantly reduces fraudulent activities such as proxy attendance and improves overall system reliability. The system architecture described in the paper includes fingerprint sensors, a microcontroller, and a database for storing user information. When a user places a finger on the sensor, the system captures the fingerprint and compares it with stored templates to verify identity. The research also evaluates the performance of the system in terms of accuracy, speed, and reliability. Results show that the fingerprint-based system provides a more efficient and secure solution compared to traditional attendance methods, making it suitable for educational institutions and organizations.

Paper Name: Study on Introducing Biometric Fingerprint Authentication in Automated Student Attendance System
Year: 2021
Publication / Journal: New Visions in Science and Technology (Book Chapter, B P International)
Author: Md. Mijanur Rahman
Summary:This study explores the integration of biometric fingerprint authentication into automated attendance systems used in academic environments. The author explains that manual attendance methods are inefficient and prone to manipulation, especially in large classrooms or universities where tracking attendance becomes challenging. The research proposes a fingerprint-based system that identifies students based on unique fingerprint minutiae features and records attendance automatically after successful verification.

The paper also discusses the technical process involved in fingerprint enrollment and authentication. During the registration phase, the fingerprint data of each student is captured and stored in a system database. When students attend a class or exam, their fingerprints are scanned and compared with stored data to confirm identity. The research findings show that biometric attendance systems provide better security, reduce administrative workload, and help institutions maintain accurate attendance records.

DOI: 10.48175/568

Paper Name: A Review Paper: Fingerprint Based Attendance System Using NodeMCU
Year: 2023
Publication / Journal: International Conference on Computing Sciences (ICCS 2023)
Authors: Archie Sinha, Rajnish Kumar Singh, Harsh Bhardwaj, Bansh Kumar Vatsa, Priyanshu Singh, Satwinder Kaur
Summary: This review paper presents an overview of fingerprint-based attendance systems developed using NodeMCU microcontrollers. The authors discuss how traditional paper-based attendance systems are outdated and inefficient, especially in institutions with a large number of students. The study highlights the benefits of adopting biometric solutions, particularly fingerprint recognition, to improve the reliability and efficiency of attendance management systems.

The paper also reviews several implementations of biometric attendance systems and evaluates their performance, cost, and usability. According to the authors, fingerprint-based systems provide a secure way of verifying individuals because fingerprints are unique and difficult to replicate. The research concludes that integrating microcontrollers like NodeMCU with fingerprint sensors and IoT technologies can help develop smart and automated attendance systems for educational institutions and organizations.

Paper Name: Biometric Fingerprint for Attendance System
Year: 2020
Publication / Journal: Research Study / Academic Publication
Authors: Sathya Durairaj, R. Vallarasu, Gomathi Sankar, K. Ajay
Summary:

This paper discusses the role of biometric fingerprint technology in modern attendance systems and security applications. The authors explain that fingerprint recognition is one of the oldest and most reliable biometric identification methods used in various sectors, including security systems, forensic analysis, and attendance monitoring. The study emphasizes that biometric systems are designed to uniquely identify individuals, ensuring accurate authentication and reducing the risk of identity fraud.

The research also highlights the technical challenges involved in fingerprint matching, such as distortion or variations in fingerprint images during scanning. Despite these challenges, the system demonstrates strong performance in verifying user identities when proper algorithms and sensors are used. The paper concludes that fingerprint-based attendance systems are highly effective in improving the accuracy and security of identification processes in educational and organizational environments.

Paper Name: Evaluating the Effectiveness and Performance of an Examination Hall Attendance System with High-Performance Face Recognition and Fingerprint Technology
Year: 2025
Publication / Journal: International Journal of Science Research and Technology Authors: Isah Abdullahi Wapanda, Aliyu Buba Dahiru Summary: This research evaluates an advanced examination hall attendance system that combines face recognition and fingerprint authentication technologies. The authors point out that traditional methods such as manual roll calls are prone to human errors and security issues, which can negatively affect academic integrity. The proposed system integrates biometric technologies to improve the accuracy and reliability of student identification during examinations.

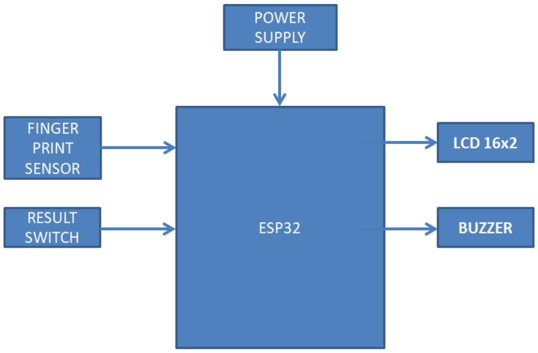
The study also analyzes system performance by comparing biometric verification with conventional attendance methods. Experimental results show that biometric-based authentication significantly reduces impersonation and improves verification speed in examination environments. The research concludes that combining multiple biometric techniques can enhance the effectiveness of examination monitoring systems and provide a more secure academic environment.

DOI: 10.48175/568

Paper Name: Optical Fingerprint-Based Attendance System Using NodeMCU ESP32
Year: 2022
Publication / Journal: Jurnal Ampere
Authors: Niksen Alfarizal, Amperawan Amperawan, Sabilal Rasyad, Khoirotun Uswa, Mourinda Nuranisah Summary: This paper presents the development of an attendance system using an optical fingerprint sensor integrated with a NodeMCU ESP32 microcontroller. The authors explain that fingerprint sensors are reliable and accurate tools for capturing biometric data and can replace manual attendance methods that are prone to mistakes. The system records attendance by scanning fingerprints and displaying the result on an LCD screen while storing data in memory for future use.

The study also discusses the advantages of integrating microcontrollers with biometric devices to create an automated and secure attendance system. By using the ESP32 platform, the system can process fingerprint data efficiently and provide real-time feedback to users. The research concludes that fingerprint-based systems improve security, simplify attendance tracking, and can be applied in schools, universities, and other organizations requiring reliable identity verification.

V. PROPOSED SYSTEM



Finger print based exam hall authentication system

Fig 1: Block Diagram

The proposed Finger Print Based Exam Hall Authentication System is developed to provide a secure and automated method for verifying student identity before allowing entry into the examination hall. The system uses biometric fingerprint technology to ensure accurate identification and prevent impersonation during examinations. It integrates hardware components such as a fingerprint sensor, ESP32 microcontroller, LCD display, and buzzer with a database system to perform authentication and attendance recording efficiently. The main goal of this system is to reduce manual verification work, improve security, and maintain accurate attendance records in a digital format.

A. System Overview

The proposed Finger Print Based Exam Hall Authentication System is designed to provide a secure and automated method for verifying students before they enter the examination hall. The system uses biometric fingerprint technology to ensure accurate identification and reduce the chances of impersonation during examinations. In this system, each student is registered in advance, and their fingerprint data is stored in a database along with their personal information. During the examination process, students authenticate themselves by placing their finger on the fingerprint scanner installed at the entrance of the exam hall. The system quickly verifies the fingerprint and determines whether the student is authorized to enter. This automated approach improves efficiency, reduces manual work for invigilators, and

DOI: 10.48175/568

helps manage large numbers of students in a systematic manner while maintaining security and reliability in the examination process.

B. Registration Module

The registration module is an important part of the proposed system because it is responsible for collecting and storing student information. In this stage, the administrator enters the details of each student, such as their name, roll number, department, and other required information. At the same time, the fingerprint sensor captures the fingerprint of the student and converts it into a digital template that represents unique fingerprint patterns. This template is then stored securely in the system database along with the student's identification details. The registration process is usually carried out before the examination period begins so that all students are properly enrolled in the system. Once the data is stored, it can be used repeatedly for authentication during examinations without requiring students to register again.

C. Authentication Module

The authentication module is responsible for verifying the identity of students when they arrive for the examination. When a student reaches the exam hall entrance, they are required to place their finger on the fingerprint sensor. The sensor scans the fingerprint and sends the captured data to the ESP32 microcontroller for processing. The microcontroller compares the scanned fingerprint with the stored fingerprint templates in the database using a matching process. If the fingerprint matches the stored record, the system confirms the identity of the student and allows entry into the examination hall. If the fingerprint does not match any stored data, the system denies access and alerts the invigilator. This module ensures that only authorized students are permitted to appear for the exam and helps prevent proxy attendance or impersonation.

D. Attendance Management Module

The attendance management module plays a significant role in maintaining accurate records of student participation in examinations. After successful authentication, the system automatically records the attendance of the student in the database. This includes important details such as the student's identity, date of the examination, and the exact time when the authentication was completed. The automated attendance recording eliminates the need for manual entry and reduces the chances of human error. It also allows administrators to easily access attendance data whenever required. The stored records can be used to generate reports, verify student participation, and maintain proper documentation for academic purposes.

E. Hardware Components

The proposed system includes several hardware components that work together to perform authentication and monitoring tasks effectively. The fingerprint sensor is used to capture the fingerprint image of students and convert it into digital data that can be processed by the system. The ESP32 microcontroller acts as the central processing unit that manages communication between all the components and performs fingerprint matching operations. A 16×2 LCD display is used to provide real-time messages to students and invigilators, such as instructions to place a finger on the sensor or displaying authentication results like access granted or denied. A buzzer is also included in the system to provide an audible alert when an unauthorized fingerprint is detected or when there is an authentication failure. These hardware components collectively ensure the smooth operation of the authentication system.

F. Working Process of the System

The working process of the system begins with the registration of student data and fingerprint templates in the database. On the day of the examination, students approach the authentication system installed at the entrance of the exam hall and place their finger on the fingerprint scanner. The sensor captures the fingerprint and sends it to the ESP32 microcontroller for verification. The system compares the scanned fingerprint with the stored templates to check for a match. If the fingerprint matches the stored data, the system grants access and records the student's attendance automatically. If the fingerprint does not match, the system denies entry and activates the buzzer to notify the invigilator about an unauthorized attempt. This process takes only a few seconds and ensures that the verification process is both quick and accurate.

G. Benefits of the Proposed System

The proposed Finger Print Based Exam Hall Authentication System offers several advantages for educational institutions. It enhances the security of the examination process by ensuring that only registered students can enter the exam hall. The system also reduces the workload of invigilators by automating the authentication and attendance recording processes. Additionally, digital storage of attendance data improves record management and makes it easier to retrieve information whenever needed. The system provides a fast and reliable method of identification, which is particularly useful in institutions where a large number of students participate in examinations. With future improvements, the system can be integrated with advanced technologies such as cloud storage, smart campus systems, and real-time monitoring platforms to further improve its efficiency and scalability.

H. Database and Data Management

The database and data management section is an important part of the proposed Finger Print Based Exam Hall Authentication System because it is responsible for storing and organizing all the information related to students and authentication records. In this system, the database stores details such as student name, roll number, department, fingerprint template, authentication status, and attendance records. During the registration phase, the fingerprint data captured by the sensor is converted into a digital template and saved in the database along with the student's personal information. This stored data acts as the reference for verifying the identity of students during the examination process. The database is designed in such a way that it can handle multiple student records efficiently and provide quick access whenever verification is required.

VI. SYSTEM DESIGN

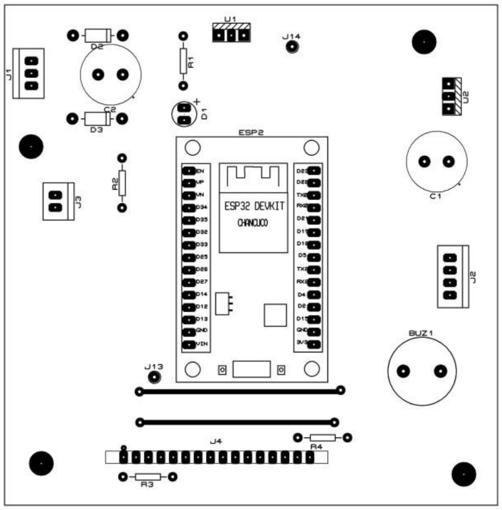


Fig 2: System Overview

The system design describes the structure, components, and workflow of the proposed Artificial Intelligence for Intelligent Decision-Making System. It explains how different modules interact with each other to collect data, process it, analyze it using AI techniques, and generate intelligent decisions. The design ensures that the system works efficiently, handles large datasets, and produces reliable outputs. A well-structured system design also improves system performance, scalability, and maintainability.

A. Overall System Architecture

The system design of the Finger Print Based Exam Hall Authentication System focuses on creating a structured and reliable framework that connects all hardware and software components to perform secure student verification. The architecture consists of a fingerprint sensor, ESP32 microcontroller, LCD display, buzzer, power supply, and a database for storing student information. These components work together to capture fingerprint data, process authentication requests, and display the verification results. The ESP32 microcontroller acts as the central unit that coordinates communication between the fingerprint sensor and the output devices. When a fingerprint is scanned, the sensor sends the captured data to the microcontroller, which compares it with stored templates in the database. Based on the comparison result, the system either grants or denies access. This architecture ensures that the authentication process is quick, accurate, and secure.

B. Hardware Design

The hardware design of the system includes all physical components required to implement the authentication process. The fingerprint sensor is responsible for capturing the biometric data of students. It reads the fingerprint patterns and converts them into digital information that can be processed by the system. The ESP32 microcontroller is used as the main controller because of its high processing capability and support for communication between devices. It manages fingerprint matching, controls system operations, and updates attendance records.

A 16×2 LCD display is used to provide visual feedback to students and administrators. It shows instructions such as placing a finger on the scanner and also displays the authentication result. The buzzer acts as an alert mechanism that is activated when an unauthorized fingerprint is detected or when verification fails. The system also includes a stable power supply unit that ensures continuous operation of all components during the examination process. Proper hardware integration is important to ensure that the system operates smoothly and provides reliable results.

C. Software Design

The software design of the system focuses on managing fingerprint enrollment, authentication, and attendance recording. The system software is programmed to control the operations of the ESP32 microcontroller and coordinate the interaction between hardware components. During the registration stage, the software captures fingerprint data and stores it in the database as a digital template. Each template is linked with the student's personal information, which helps in identifying the student during the authentication process.

When a fingerprint is scanned, the software performs a comparison between the captured fingerprint and the stored templates. This matching process determines whether the student is authorized to enter the examination hall. If a match is found, the system records attendance and displays a confirmation message. If no match is found, the system denies access and activates the buzzer. The software is designed to ensure fast processing and accurate matching to avoid delays during examinations.

D. Database Design

The database design is responsible for organizing and managing all student records and authentication data. It stores important details such as student ID, name, roll number, department, fingerprint templates, and attendance records. The database is structured in a way that allows easy retrieval of information during the authentication process.

When a student scans their fingerprint, the system quickly searches the database for a matching template.

In addition to storing fingerprint data, the database also keeps track of attendance history and authentication logs. This helps administrators analyze attendance patterns and maintain proper records of examination participation. A well-

DOI: 10.48175/568

designed database ensures that the system can handle large numbers of student records efficiently without affecting system performance.

E. Data Flow Design

The data flow design explains how information moves within the system during operation. The process begins when a student places their finger on the fingerprint sensor. The sensor captures the fingerprint image and converts it into digital data. This data is then transmitted to the ESP32 microcontroller for processing. The microcontroller checks the database for a matching fingerprint template and verifies the identity of the student.

After verification, the result is sent to the output devices such as the LCD display and buzzer. If the authentication is successful, the system records the attendance and displays a confirmation message. If authentication fails, the system displays a denial message and triggers an alert. This continuous flow of data between components ensures that the system operates efficiently and provides quick responses during the examination process.

F. Security Design

Security is a key aspect of the system design because the system handles sensitive biometric data. The system is designed to store fingerprint templates instead of raw fingerprint images to protect user privacy. Access to the database is restricted to authorized administrators to prevent unauthorized modification of records. The authentication process is also designed to detect invalid attempts and alert the invigilator through the buzzer.

In addition, the system maintains logs of authentication activities, which can be used for monitoring and auditing purposes. By implementing proper security measures, the system ensures that biometric data is handled safely and that the examination process remains fair and transparent.

G. System Operation Flow

The overall operation of the system follows a structured sequence of steps to ensure proper authentication. Initially, students are registered in the system along with their fingerprint data. During the examination, students approach the authentication device and scan their fingerprint. The system processes the fingerprint data and compares it with stored records in the database. If a match is found, the system grants access and records attendance automatically. If the fingerprint does not match any record, the system denies entry and alerts the invigilator. This systematic flow of operations ensures smooth functioning of the system and minimizes delays during student verification.

VII. HARDWARE COMPONANT

1. Fingerprint Sensor

Fig 3: Fingerprint Sensor

The fingerprint sensor is the main biometric input device used in the Finger Print Based Exam Hall Authentication System. Its primary function is to capture the fingerprint image of a student and convert it into digital data that can be processed by the system. When a student places their finger on the sensor, it scans the unique patterns such as ridges and valleys present on the fingerprint surface. These patterns are then analyzed and converted into a digital template that represents the unique identity of the individual. The sensor also performs basic preprocessing such as image enhancement and feature extraction to ensure accurate recognition. During authentication, the sensor captures a new fingerprint image and sends it to the microcontroller for comparison with stored templates in the database. Because fingerprints are unique to every individual, this component plays a critical role in ensuring accurate identity verification and preventing impersonation during examinations.

2. ESP32 Microcontroller

Fig 4: ESP32 Microcontroller

The ESP32 microcontroller acts as the central processing unit of the entire authentication system. It is responsible for controlling and coordinating all the hardware components connected to the system. When the fingerprint sensor captures fingerprint data, the ESP32 receives this data and performs the verification process by comparing it with stored fingerprint templates. In addition to authentication, the microcontroller also manages system operations such as displaying messages on the LCD screen, activating the buzzer during unauthorized access attempts, and updating attendance records in the database. The ESP32 is widely used in embedded systems because it offers high processing speed, low power consumption, and built-in communication capabilities such as Wi-Fi and Bluetooth. These features allow the system to operate efficiently and provide quick authentication results, making it suitable for examination environments where many students need to be verified in a short period of time.

3. LCD Display (16×2)

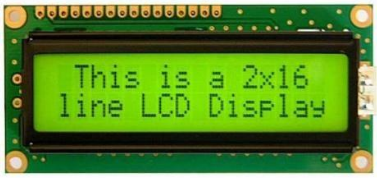


Fig 5: LCD Display (16×2)

The LCD display is used as the output interface of the system to provide real-time information to students and administrators. It helps guide users during the authentication process by showing messages such as “Place Finger,” “Access Granted,” or “Access Denied.” This display makes the system user-friendly and easy to understand, even for individuals who are not familiar with biometric systems. When the authentication process is completed, the LCD shows the verification result immediately, allowing students and invigilators to know whether the student is authorized to enter the examination hall. In addition, the display can also show system status messages, error notifications, or instructions during the registration process. By providing clear visual feedback, the LCD display improves the interaction between the user and the authentication system.

4. Buzzer

Fig 6: Buzzer

The buzzer is an alert device used in the system to provide an audible signal when certain events occur, especially during authentication failures or unauthorized access attempts. If a fingerprint does not match any stored record in the database, the buzzer is activated to notify the invigilator or administrator immediately. This helps in quickly identifying suspicious activity or potential impersonation cases. The buzzer also enhances the overall security of the system by drawing attention to authentication errors or system warnings. In examination environments where many students are entering the hall, the buzzer ensures that any irregular activity is not overlooked. This component works alongside the LCD display to provide both visual and audio notifications for better system monitoring.

5. Database

The database is responsible for storing all important information related to students and authentication records. It contains details such as student names, roll numbers, departments, fingerprint templates, and attendance records. During the registration phase, the fingerprint data captured by the sensor is converted into a digital template and stored in the database along with the student's personal details. When authentication takes place, the system retrieves the stored fingerprint template and compares it with the scanned fingerprint to verify identity. The database also records attendance automatically after successful authentication, including the date and time of entry into the examination hall. Proper database management ensures that records are stored securely and can be accessed easily when needed for reporting or monitoring purposes.

6. Power Supply Unit

Fig 7: Power Supply Unit

The power supply unit is an essential component that provides the required electrical power to all parts of the system, including the fingerprint sensor, ESP32 microcontroller, LCD display, and buzzer. A stable and reliable power source is necessary to ensure that the system operates continuously during examination periods without interruption. If the power supply is unstable, it may affect the performance of the system and cause delays or errors during authentication. Therefore, the power supply unit is designed to provide consistent voltage and protect the system components from electrical fluctuations. In some implementations, backup power options such as batteries or uninterrupted power supply systems can also be used to maintain system operation even during power outages.

7. Result Switch / Control Button

The result switch or control button is used to initiate or control certain operations within the authentication system. It allows the administrator or invigilator to manage the system during registration or authentication processes. For example, the switch can be used to start the fingerprint scanning process, confirm data entry, or reset the system when required. This component ensures that the system can be operated easily and provides manual control when necessary. Although the system is largely automated, the presence of a control switch allows administrators to manage system functions efficiently during examinations or system setup.

Circuit diagram

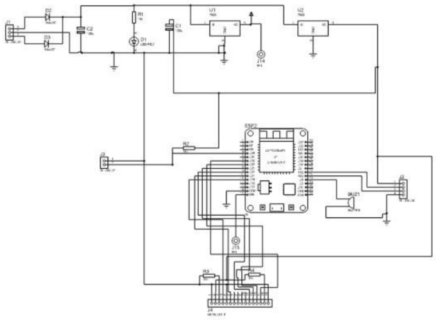


Fig 8: Circuit diagram

PCB Layout

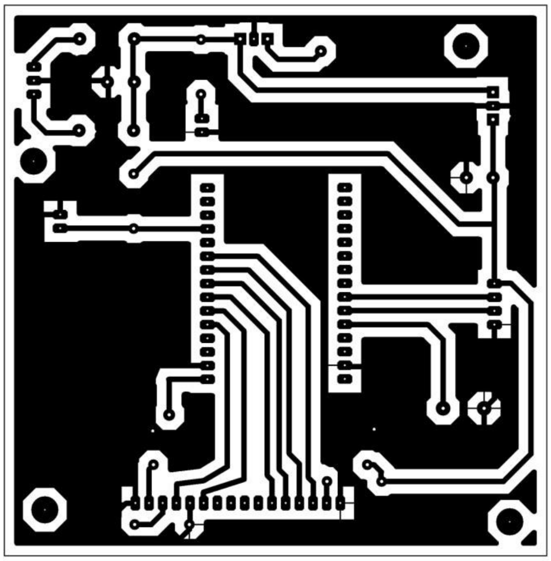


Fig 9: PCB Layout

VIII. RESULT

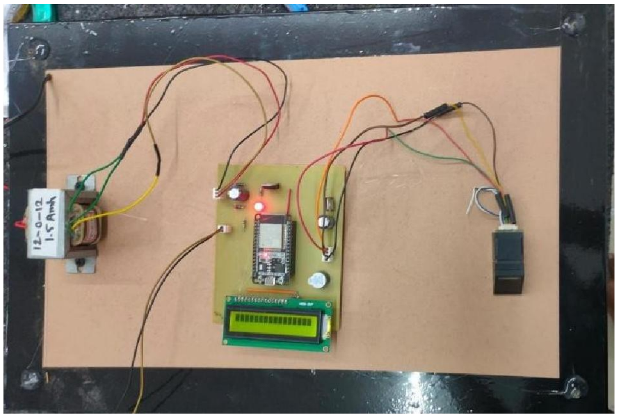


Fig 10: Result

This image shows a hardware prototype setup of an embedded system project mounted on a baseboard. The system appears to be designed for control and display purposes using a microcontroller.

At the center of the setup is a microcontroller development board (likely an ESP or Arduino-based module) mounted on a printed circuit board (PCB). It is connected with multiple jumper wires for power and signal transmission. A glowing red LED indicates that the system is powered and actively running.

Below the microcontroller, there is a 16x2 LCD display module. This display is typically used to show real-time data such as sensor readings, system status, or user messages. Although the content on the screen is not clearly visible, its presence suggests that the system provides output feedback to the user.

On the left side of the setup, a step-down transformer is connected, which likely converts high voltage AC supply to a lower voltage suitable for the circuit. This indicates that the system is powered through an external electrical source. On the right side, there is a small DC motor connected via wires. This motor may be used as an output actuator, controlled by the microcontroller based on programmed logic or sensor input. A small cylindrical component (possibly a capacitor or sensor) is also visible near the controller, which may be used for filtering or sensing purposes.

Overall, the image represents a working prototype of an embedded system that integrates power supply, processing unit, display module, and output device (motor). It demonstrates practical implementation of electronics and programming concepts, commonly used in automation or control-based applications.

Graph 2: Average Verification Time by Method

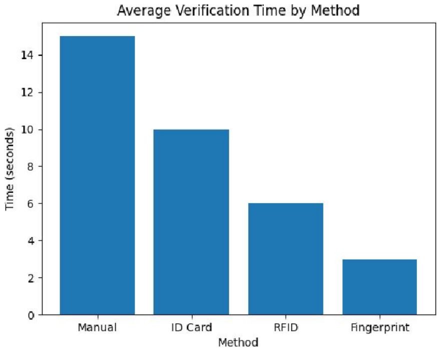


Fig 11: Graph 1

This graph compares the time required for student verification using different methods such as manual checking, ID card verification, RFID systems, and fingerprint authentication. The results clearly show that the fingerprint-based

DOI: 10.48175/568

authentication system requires less time compared to traditional methods. Manual verification takes the longest time because it involves checking documents and verifying student identity manually.

The fingerprint authentication method is faster because the system automatically scans and verifies the fingerprint within a few seconds. This reduces waiting time at the entrance of the examination hall and helps manage large numbers of students more efficiently.

Table 2: Verification Time Comparison

Verification Method	Time Required (Seconds)
Manual Verification	15
ID Card Checking	10
RFID System	6
Fingerprint Authentication	3

Graph 3: Unauthorized Attempts Detected During Exams

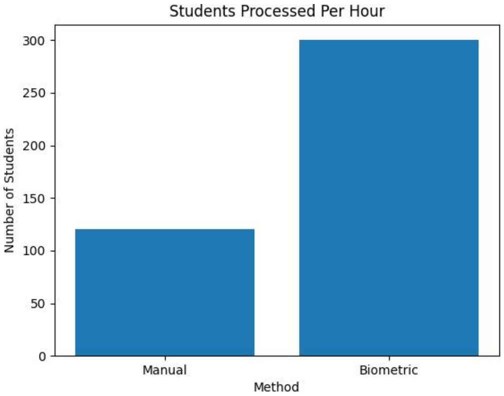


Fig 12: Graph 2

This graph illustrates the number of unauthorized access attempts detected by the system during different examination days. The results indicate that the number of unauthorized attempts decreases over time. This happens because students become aware that the system uses biometric authentication, which prevents impersonation and proxy attendance.

The presence of a buzzer alert and strict verification process helps invigilators monitor suspicious activities effectively. As a result, the system improves the overall security of the examination environment.

Table 3: Unauthorized Access Attempts

Exam Day	Unauthorized Attempts
Day 1	5
Day 2	4
Day 3	3
Day 4	2
Day 5	1

DOI: 10.48175/568

Graph 4: Attendance Processing Efficiency

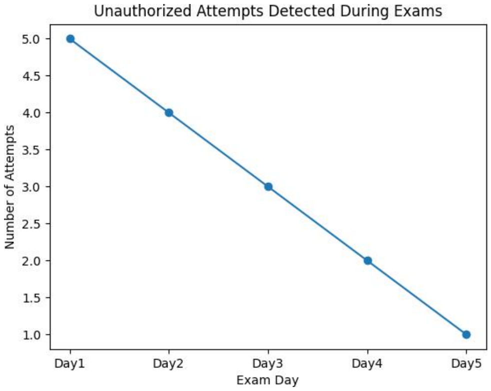


Fig 13: Graph 3

This graph shows the number of students processed per hour using manual attendance and the proposed biometric system. The results demonstrate that the fingerprint-based system can handle a larger number of students in a shorter period of time. Manual attendance methods require more time because invigilators must verify each student individually.

In contrast, the biometric system quickly verifies student identity and records attendance automatically. This significantly increases efficiency and reduces congestion at the exam hall entrance.

Method	Students Processed per Hour
Manual Method	120
Biometric System	300

IX. CONCLUSION

The Finger Print Based Exam Hall Authentication System provides a reliable and modern solution for improving the security and efficiency of student verification during examinations. Traditional methods such as manual attendance and ID card checking often lead to delays, errors, and the possibility of impersonation. By introducing biometric authentication through fingerprint recognition, the proposed system ensures that each student is accurately identified before entering the examination hall. This approach not only strengthens the credibility of the examination process but also helps educational institutions maintain fairness and transparency.

The system integrates a fingerprint sensor with an ESP32 microcontroller, which works as the central processing unit responsible for capturing, analyzing, and verifying fingerprint data. Supporting components such as an LCD display and buzzer provide real-time feedback and alerts, making the system easy to operate and monitor. The automated attendance recording feature reduces the workload of invigilators and ensures that all records are stored digitally and accurately. As a result, the system improves both operational efficiency and data management in examination environments.

Another important advantage of the proposed system is its ability to reduce unauthorized access and prevent proxy attendance. Since fingerprints are unique for every individual, the system offers a highly secure method of identification compared to traditional approaches. The results obtained from system testing demonstrate that the authentication process is fast, accurate, and capable of handling large numbers of students effectively. This makes the system suitable for colleges, universities, and examination centers that require reliable identity verification.

X. FUTURE SCOPE

The Finger Print Based Exam Hall Authentication System has strong potential for further development and improvement as technology continues to advance. Although the current system provides secure authentication and

DOI: 10.48175/568

automated attendance management, additional features and enhancements can make it more efficient, scalable, and suitable for large educational institutions. Future improvements can focus on integrating advanced technologies that enhance system performance, data management, and user convenience.

One possible improvement is the integration of cloud- based storage and monitoring systems. By connecting the authentication system to a cloud platform, institutions can store attendance records and authentication data securely and access them from multiple locations. This would allow administrators to monitor examination activities in real time and generate reports easily. Cloud integration would also help in maintaining backup data and reducing the risk of data loss.

Another important future development is the combination of multiple biometric authentication methods. In addition to fingerprint recognition, the system can be expanded to include facial recognition, iris scanning, or smart card verification. Using multiple authentication techniques can increase the reliability of the system and reduce the chances of authentication failure. This approach can also provide alternative verification methods in situations where fingerprint recognition may not work properly due to technical or physical conditions.

The system can also be improved by developing a mobile and web-based management application for administrators and examination authorities. Through such applications, administrators can manage student records, monitor attendance, and receive notifications about authentication activities. This would make the system more flexible and easier to manage, especially in institutions with multiple examination centers.

REFERENCES

1) P. Chandra Sekhar, B. Anagani, Reshmi, Aruna, and S. Priya, “Fingerprint Based Exam Hall Authentication,” International Journal for Research in Applied Science and Engineering Technology (IJRASET), 2023.

2) S. Chandra Sekhar, Y. B. N., Yashas R., Lohith K. N., and Tejas N., “Fingerprint-Based Exam Hall Authentication Using IoT,” Journal of Advancement in Electronics Signal Processing, 2024.

3) Md. Mijanur Rahman, “Study on Introducing Biometric Fingerprint Authentication in Automated Student Attendance System,” in New Visions in Science and Technology, B P International, 2021.

4) N. Alfarizal, A. Amperawan, S. Rasyad, K. Uswa, and
M. Nuranisah, “Optical Fingerprint-Based Attendance System Using NodeMCU ESP32,” Jurnal Ampere, 2022.

5) I. A. Wapanda and A. B. Dahiru, “Evaluating the Effectiveness and Performance of an Examination Hall Attendance System with Face Recognition and Fingerprint Technology,” International Journal of Science Research and Technology, 2025.

6) O. J. Adetunji, M. Sanni, E. Noma-Osaghae, A. I. Oyedeji, and O. V. Bello, “Design and Implementation of Face Attendance Recognition System Using ESP32- CAM,” FUW Trends in Science & Technology Journal, 2025.

7) R. Chavan, V. J. Badale, O. K. Chavan, V. P. Dahiphale, and S. B. Gaikwad, “Real Time Attendance System Using ESP32,” Journal of Propulsion Technology, 2024.

8) S. Medhavath, M. Modium, P. Pasula, and D. Begari, “Face Recognition Based Attendance System Using ESP32CAM,” International Journal of Engineering Applied Sciences and Technology, 2023.

9) A. Yadav, P. Dalvi, and H. Juwale, “RFID-Based Attendance Management System Using ESP32 and Google Sheets,” The Voice of Creative Research, 2025.

10) F. Demenschonok, J. Harrigan, and T. Bonaci, “An Overview of Fingerprint-Based Authentication: Liveness Detection and Beyond,” arXiv preprint arXiv:2001.09183, 2020.

11) J. M. Singh, A. Madhun, G. Li, and R. Ramachandra, “A Survey on Unknown Presentation Attack Detection for Fingerprint Recognition Systems,” arXiv preprint arXiv:2005.08337, 2020.

12) H. Li and R. Ramachandra, “Deep Learning Based Fingerprint Presentation Attack Detection: A Comprehensive Survey,” arXiv preprint arXiv:2305.17522, 2023.

13) J. Ramakrishnan and M. Ramakrishnan, “An Efficient Automatic Attendance System Using Fingerprint Reconstruction Technique,” arXiv preprint arXiv:1208.1672, 2012.

14) K. Jain, A. Ross, and S. Prabhakar, “An Introduction to Biometric Recognition,” IEEE Transactions on Circuits and Systems for Video Technology, 2004.

15) N. K. Ratha and R. M. Bolle, Automatic Fingerprint Recognition Systems, Springer, 2004.

16) D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer, 2009.

17) A. K. Jain, A. Ross, and K. Nandakumar, Introduction to Biometrics, Springer, 2011.

18) M. K. Sharma and R. Gupta, “Biometric Based Student Attendance System,” International Journal of Computer Applications, 2018.

19) S. Patil and V. Pawar, “Fingerprint Based Attendance System Using Microcontroller,” International Journal of Engineering Research and Technology, 2019.

20) P. Verma and S. Singh, “Design and Implementation of Biometric Attendance System,” International Journal of Advanced Research in Computer Engineering and Technology, 2020..