

Development Of An Esp32-Microcontroller-Based Biometric System For Classroom Management

Gabriel Ebiowei Moses¹, Ayibepreye B. Kelvin², David Ebregbe³

gabrielebiowei@ndu.edu.ng

Department of Electrical and Electronics Engineering, Niger Delta University, Bayelsa, Nigeria

ABSTRACT: The increasing difficulty associated with the proper administration of examinations in tertiary institutions, identity theft, impersonation, falsification and manipulation of attendance records, absenteeism on the part of lecturers and students and several other related security issues plaguing our university communities is of grave concern. This paper presents the “Development of an ESP32-Microcontroller-Based Biometric System for Classroom Management”. It proposes a novel attendance and classroom management system leveraging the ESP32 microcontroller and the unique biometrics of individuals. The ESP32 microcontroller, with its built-in Wi-Fi and Bluetooth capabilities, enables seamless connectivity and data transfer. The system consists of a fingerprint sensor, ESP32 board, and a web-based interface. Students' fingerprints are enrolled and stored in the database, allowing for secure and accurate identification. The web interface enables administrators to monitor attendance, lecturer's promptness/regularity in class, and track student activity. After rigorous tests, the results obtained show that: - Image acquisition time gives 0.5 seconds, - False Acceptance Rate (FAR) is 0.2%, etc. The system demonstrated high accuracy and efficiency, with rapid image acquisition and low error rates. The FAR and FRR results indicate a high level of security and reliability, ensuring that only registered students can access the classroom and that legitimate students are not denied access. This system offers numerous benefits, such as: Improved attendance accuracy and reduced fraud, Reduced administrative burdens and increased efficiency, and real-time insights into students and lecturers' attendance patterns. This paper provides a foundation for further research and development in this area, including the integration of additional functionalities such as multiple fingerprints and the exploration of other biometric modalities.

KEYWORDS: ESP 32 Microcontroller, Sensors, Classroom Management, Biometric Systems, Fingerprints, Web Interface, Database Management.

INTRODUCTION

Recording and keeping track of student attendance is mandatory in an educational institute. Updating and maintaining those attendances plays a vital role in administration and accounting. Accurately tracking attendance has become a critical need for many organizations across both public and private sectors. Educational institutions require reliable attendance logs for meeting regulatory compliance (Scott, 2015), improving student outcomes through analysis of participation trends and calculating resources allocations. Corporate offices and other workplaces aim to closely monitor hourly employee attendance tied to payroll, account for vacation/sick time, and analyze usage patterns of facilities and resources.

Recognizing the limitations of conventional attendance tracking systems, there is an increasing demand for more secure, accurate, and automated alternatives. Biometric technology has emerged as a robust solution for identity verification, and its integration into attendance management systems promises enhanced precision and reliability. Fingerprint-based biometric tracking offers a highly accurate automated approach to recording attendance data while linking unambiguously to member identities (Pugliese, 2016).

The integration of microcontrollers with fingerprint recognition technology represents a synergistic approach that not only yields a sophisticated but also a cost-effective solution to the challenges faced by traditional attendance management systems (Tarmissi et al, 2024). Microcontrollers, characterized by their compact design and versatile capabilities as integrated circuits, contribute significantly to the development of an advanced system that seamlessly combines security, efficiency, and affordability. Microcontrollers serve as the central intelligence of the system, orchestrating the various tasks required for efficient attendance management (Gadade et al, 2024).

These compact devices excel at processing and managing data, offering a powerful computational backbone for the fingerprint recognition technology to operate seamlessly. Their ability to execute tasks swiftly and reliably makes them ideal for handling the complex algorithms involved in fingerprint matching and verification. Furthermore, microcontrollers exhibit a remarkable adaptability to interface with diverse hardware components (Dong et al, 2020).

This versatility allows them to connect effortlessly with fingerprint sensors, display units, connectivity modules, and other essential elements of the attendance management system. Such integration creates a cohesive ecosystem where each component functions harmoniously under the governance of the microcontroller, ensuring a well-coordinated and synchronized operation. The streamlined approach facilitated by microcontrollers in attendance management is particularly noteworthy. The automation of processes, from capturing fingerprints to storing and processing data, significantly reduces the need for manual intervention (Moses et al, 2011).

This not only enhances the overall efficiency of the system but, also mitigates the inherent risks of inaccuracies associated with traditional methods. By minimizing human involvement, the system becomes less susceptible to errors caused by manual data entry

or manipulation, fostering a more dependable and secure environment for attendance tracking. Moreover, the cost-effectiveness of the solution is a direct result of the efficiency and scalability offered by microcontrollers. Their relatively low cost, coupled with their ability to handle complex tasks, contributes to the affordability of implementing a microcontroller-based fingerprint attendance management system (Ahsan. 2006).

By adopting this Microcontroller-based Biometric Attendance and Classroom Management System, organizations stand to streamline their administrative processes significantly. Automation of attendance tracking not only reduces the burden on administrative personnel but also minimizes the scope for human error (Budiarto, M. et al, 2024). The overall impact extends beyond mere attendance tracking. Improved accuracy and efficiency in record-keeping contribute to enhanced organizational efficiency. The time and resources previously spent on manual data entry and rectification of errors can now be redirected towards more strategic tasks. This not only optimizes workforce productivity but also empowers organizations to allocate resources more judiciously, ultimately contributing to cost-effectiveness and improved resource utilization.

In essence, the Microcontroller-Based Biometric Attendance and Classroom Management System represents a paradigm shift in the way organizations approach attendance tracking and management. By marrying the precision of biometric identification with the efficiency of microcontroller technology, this system is poised to redefine standards of accuracy, security, and efficiency, thus laying the foundation for a more streamlined and productive organizational environment (Yeap, K. H. et al, 2024).

Attendance administration and control is an important requirement in various institutions as it provides a suitable documentation in record keeping, students assessment; consistency in service and defines requirement for taking part in an examination in most educational institutions (Shoewu & Idowu, 2012).

By evaluating both literature-based best practices and the practical development of a fingerprint biometric attendance system (Kadry & Smaili, 2010), this research aims to determine ideal implementation frameworks organizations can adopt in managing this critical domain. The system not only simplifies the process of taking attendance, but it also lowers faults and enables for faster confirmation of student presence, all while requiring little human intervention. The created solution should not only simplify the work but also increases the institutions efficiency in manpower and time management.

LITERATURE REVIEW

The literature review is broadly based on the following sub-headings: commonly used biometric elements, strength of biometric technology, microcontrollers for fingerprint analysis, review of empirical studies and research gap.

Commonly Used Biometric Elements

With the evolution of modern cloning techniques, the most commonly used and reliable modes of biometrics is the iris and fingerprints of individuals (Meden *et al*, 2021). I will take a critical look at the biometric element that is at the center of this research work (the fingerprint) later. Some commonly used biometric elements are shown in Figure 1.

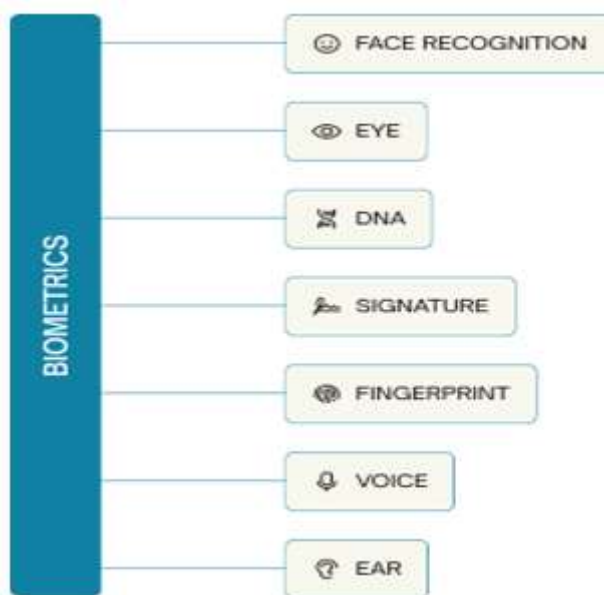


Figure 1: Schematic of commonly used biometric elements

Biometrics

Biometrics is an automated technology used for people recognition using physiological identifiers. Biometrics covers a variety of technologies in which inimitable identifiable attributes of people are used for identification and verification. These include a person's fingerprint, face, iris, voice, palm prints, which can be used to authenticate the distinctiveness of individuals. Biometric data is unique for each person so it can be used in almost any application that requires the accurate identification or verification of any individual. Fundamentally, biometrics refers to automated recognition of individuals based on distinguishing biological or behavioural traits like fingerprints, voice patterns, or facial structure (Jain et al., 2012). What makes biometrics desirable for reliable authentication stems from their unique properties. Most biometric characteristics inherently contain sufficient complexity at microscopic or sub-structural levels enabling differentiation between individuals if captured at requisite fidelities (Mehrotra et al, 2021).

Fingerprints as a biometric specifically contain ridge flow patterns, minutiae points, and other microscopic irregularities lending to distinctiveness even between identical twins when scanned accurately (Maltoni et al, 2009). This enables identity verification through matching live template scans to an existing enrolled profile using recognition algorithms. For attendance tracking then, the key premise lies in biometrically confirming a member's declared identity at system checkpoints using fingerprints as proof over manual declarations or badge proxies. By tying verification events directly to individual members, attendance logs become far less forgeable and traceable over time (Scott, 2015). Analyzing participation based on verified identities supports more credible usage assumptions, planning decisions, and accountability measures for both administrators and end users

Deoxyribonucleic Acid (DNA)

Deoxyribonucleic Acid (DNA) is the ultimate unique code for one individuality, except for the fact that identical twins have identical DNA patterns. However, it is mostly used in the context of forensic applications for person recognitions. DNA, or deoxyribonucleic acid, is one of the most fundamental and reliable biometric identifiers due to its unique and highly specific characteristics for each individual (except identical twins).

The Ear

The shape of the ear, the structure of the cartilaginous tissue of the pinna is distinctive although these features are not unique for all individuals. The ear recognition approaches are based on matching the distance of salient points on the pinna from a landmark location on the ear. The human ear can serve as an effective biometric element due to its unique anatomical features, which remain relatively unchanged over time (Bhanu & Chen 2008). There are several reasons why the ear is considered a viable biometric identifier. The unique features of the ear that makes it a viable biometric identifier are the structure, stability over time and difficulty to alter.

Facial Recognition

Facial recognition technology has gained significant attention in recent years due to its wide range of applications (Oloyede et al, 2020), from security and surveillance to user authentication and personalized marketing. There are many proprietary facial recognition software solutions. There are some few free access open source system such as OpenFace, OpenBR (Open Biometrics), DLib, and DeepFaceLab.

Signature

This technology uses the dynamic analysis of a signature to authenticate a person, the way a person signs his name is known to be a characteristic of that individual (Delac & Grgic, 2004). Although signatures require contact and effort with the writing instrument, they seem to be acceptable in many government, legal, and commercial transactions as a method of verification. Signatures are a behavioral biometric that change over a period of time and are influenced by physical and emotional conditions of the signatories thus the signature biometrics is not widely accepted.

Iris Scanning

Iris scanning represents another biometric approach leveraging the distinct visual texture patterns present in the colored muscular tissue surrounding eye pupils. While fingerprints focus on external friction ridge arrangements, irises contain more randomized trabecular meshwork formations with intricate pigmentation details (Mehrotra et al, 2021).

Voice Recognition

Voice recognition as a biometric technology for attendance systems relies on using automated analyses of a person's speech samples to verify their declared identity. Voice recognition extracts distinctive attributes within tones, range, cadences, syntax and speech patterns across individuals that algorithms encode into templates for matching purposes (Mehrotra et al, 2021). Voice recognition extracts distinctive attributes within tones, range, cadences, syntax and speech patterns across individuals that algorithms encode into templates for matching purposes (Mehrotra et al, 2021).

Vein Patterns

Vein pattern biometric systems for identity tracking, including potential attendance applications, leverage the unique structure of the complex vascular networks present beneath human skin. Near-infrared imaging techniques allow visualization of superficial blood vessels coursing through the hands, fingers or wrists as dark web-like structures in contrast to surrounding tissue based on differential absorption spectra (Mehrotra et al, 2021). Resulting imagery reveals highly intricate vascular morphology patterns containing vessel thickness variances, minutiae bifurcations/crossovers and fine termination points. Specialized extraction, segmentation and thinning algorithms can encode these characteristic vascular traits into encrypted identity templates analogous to fingerprint or iris analyses (Jain et al, 2012).

Strength of Biometric Technology

There have been a lot of advancements in the field of biometrics over the past few years, which has made it more acceptable in recent years. Biometric technology is the automatic techniques of recognizing or confirming the identity of a living person in particular cantered on a physiological or behavioural trait. The technology has proven to be more efficient over other identification technology because of its uniqueness which ensures privacy or data discretion, authorization and non-repudiation. It ensures high identification accuracy. It is also used in the forensics sector for criminal identification and prison security. It ensures fast and reliable protected access to information. Currently, techniques such as password verification have a lot of issues. Biometric has eliminated those issues and need to use password all the time.

METHODOLOGY

Several design approach including their advantages and disadvantages is explained. Brief explanatory notes and requisite manufacturers' data of some material is added to enhance quick understanding of certain technical detail-working in the hardware and circuitry. It is worthy of note that extra effort is made in the choice and application of the microcontroller. A detailed procedural design of the attendance system is explained. Among others, the methodology is based on: ESP32 microcontroller, fingerprint scanner, 20x4 LCD display with I2C pin assignments, dot matrix keypad, database software, etc. The methodology used in this research adheres strictly to the modular circuit design structure. Designing a microcontroller-based biometric device involves several steps, from conceptualization to implementation.

Materials used

1. Breadboard
2. ESP32 Microcontroller Unit

System Circuit Diagram using EPS32

Figures 2 and 3 shows the circuit diagram and implementation of the system respectively. The LCD is connected to the ESP32 by I2C, the fingerprint module via serial port, and the keypad via GPIO pins. The details are shown in the individual connection diagrams as explained in the respective modules.

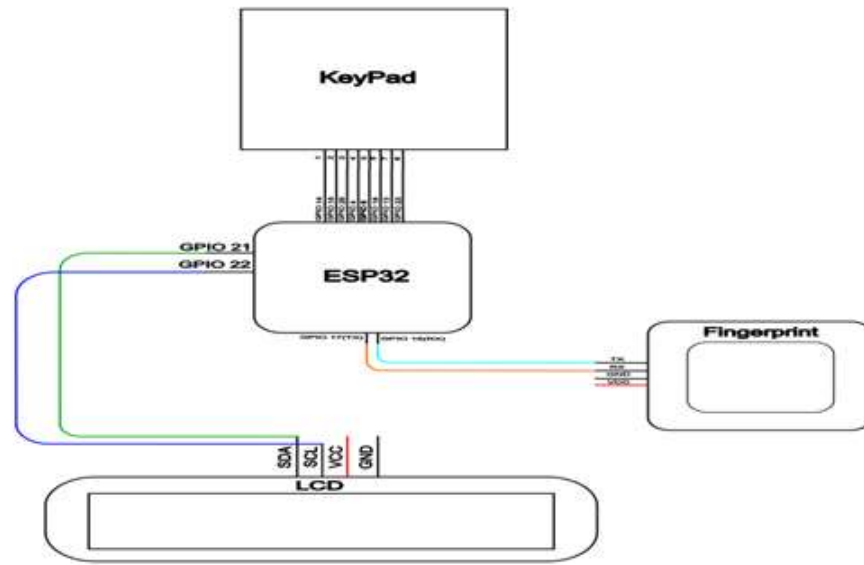


Figure 2: Complete wiring diagram of the system (Showing major hardware)

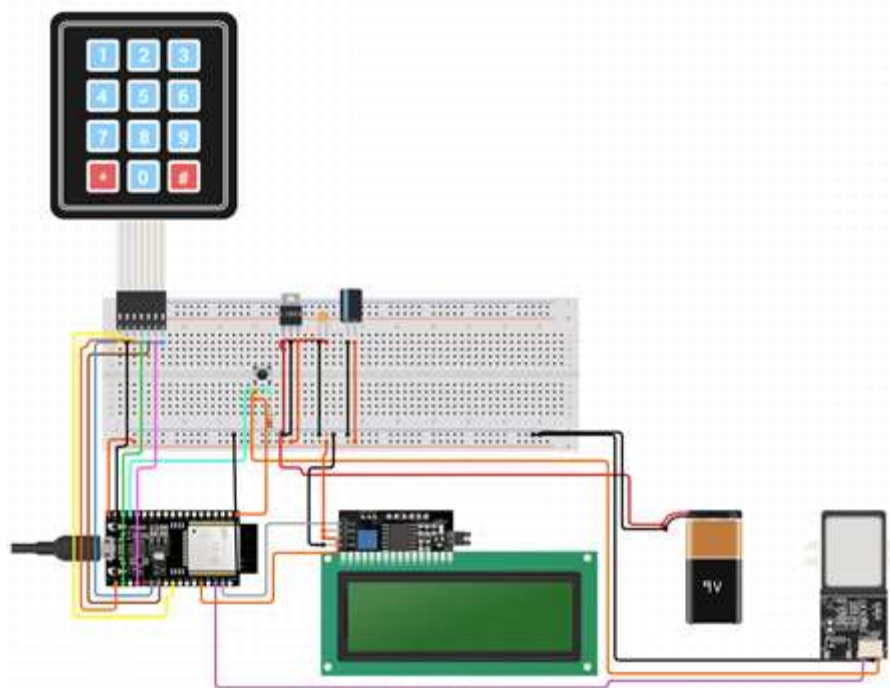


Figure 3: Breadboard assembly of the system showing the major components

ARCHITECTURE

The project follows client-server architecture:

- Client: The hardware fingerprint device (Arduino-based).
- Server: A Django web application that processes fingerprint data and manages users.
- Communication Protocol: The client and server communicate over HTTP, following a request-response model where the client sends data to the server and receives responses accordingly.

TECHNOLOGY STACK

The project is developed using:

- A. Arduino Framework for the hardware.
- B. Django Framework for the server-side application.
- C. SQLite (development) → PostgreSQL (production) for data storage.

To simplify the development process, several external libraries were used:

HARDWARE (ARDUINO)

- 1. FPM (by brianrho): Interfaces the fingerprint module with the Arduino microcontroller. Chosen over the popular Adafruit Fingerprint Library due to its ability to send fingerprint templates over serial communication or a network, which was critical for this project.
- 2. Arduino_JSON: Handles serialization and deserialization of data exchanged between the hardware and server.
- 3. LiquidCrystal_I2C: Manages the LCD display connected via I2C for user interaction.
- 4. Keypad (by Mark Stanley, Alexander Brevig): Supports input handling for the 8x8 matrix keypad used in the device.

SOFTWARE (DJANGO WEB APPLICATION)

- 1. Django ORM: Enables secure and efficient database interactions without writing raw SQL queries.
- 2. Django Admin: Provides an administrative interface for managing users and device data.
- 3. Django Ninja: Simplifies API development, offering automatic API documentation via Swagger UI.

DATA STORAGE & FINGERPRINT MANAGEMENT

- 1. User Data (Lecturers & Students):
 - i. Stored in SQLite during development.
 - ii. Switched to PostgreSQL in production for better performance and scalability.
- 2. Fingerprint Templates:
 - i. Stored as binary files in file system storage instead of a database, ensuring faster access and reducing database load.

DEVICE AND SERVER WORKFLOW

This section outlines how the IoT fingerprint device interacts with the server and explains the design choices that shaped its functionality.

ATTENDANCE WORKFLOW

When the device enters Attendance Mode, another conditional check determines whether the user is a lecturer or a student:

- Lecturers can start a course session, making it available for attendance.
- Students can only join a course session that has already been started by a lecturer, provided they are registered for that course.

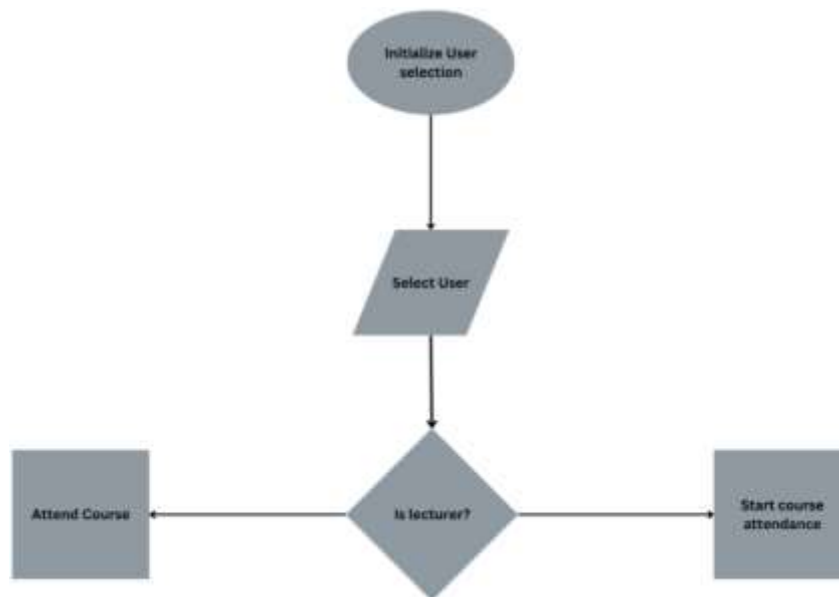


Figure 4: Attendance Work-flow, User Verification

USER VERIFICATION (FINGERPRINT AUTHENTICATION)

To verify a user's identity, the device uses the fingerprint module:

- A. Enrollment Phase:
 - i. When a user is enrolled, their fingerprint template is stored on the server.
- B. Attendance Phase:
 - i. When a user attempts to mark attendance, their fingerprint template is fetched from the server.
 - ii. The template is then stored temporarily on the fingerprint module for verification.
 - iii. If the scanned fingerprint matches the stored template, attendance is recorded successfully.

By handling fingerprint storage on the server and loading them dynamically onto the device, we ensure efficient memory usage and better scalability for multiple users.

Process Overview

This part offers a thorough overview of the system's operational process and the interaction between devices and the web application, as depicted in Figure 5. The system entails the deployment of a specific number of devices, denoted as "N," strategically positioned across various lecture halls. These devices collectively communicate with a central server, which is hosted on the internet. To ensure integrity, only registered devices are permitted to establish communication with the central server, thereby mitigating the potential for any unauthorized or improper usage.

The system consists of two processes:

- The registration processes
- Attendance management

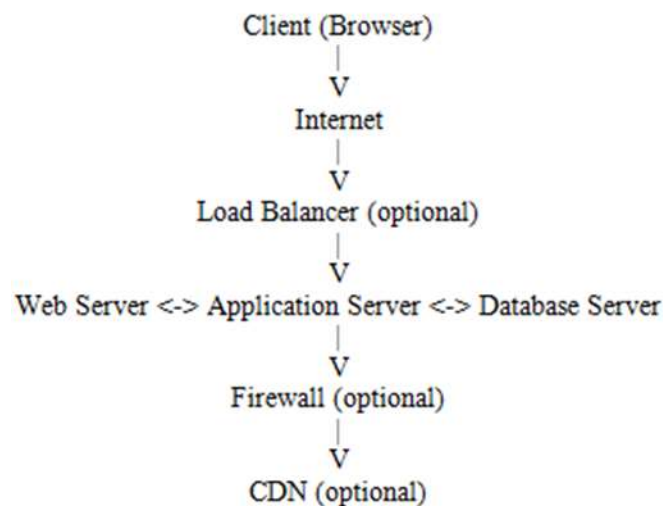


Figure 5: Schematic (Flow-drawing) representation of a web-based system

The Registration Processes

This pivotal process oversees the registration of all entities integral to the system. The system encompasses four key entities:

1. Lecturers
2. Students
3. Devices
4. Courses

Attendance Management

This is the core of the whole design. All the courses are originally uploaded in the system. Students' biodata is captured and stored in the database. Students cannot enroll for courses that are not found in the database. Lecturers are assigned course(s) and hence

have the ability to activate such course(s) for students to attend the class by placing their fingers on the scanner to be read. It is thus the attendance management system that keeps track of lecturers and students class attendance. This information is vital for management decision making. A student that didn't register for a course cannot be seen as having written an examination hence the biodata is used to record his/her attendance in any examination.

Description of the fingerprint biodata system

The system has the following features:

A. Lecturers (Academia)

- i. Register lecturers (Using password or fingerprint)
- ii. Assign course(s) to lecturers
- iii. Track lecturer's login time
- iv. Track class start time

B. Students

- i. Register students and capture (picture and) fingerprint biodata
- ii. Enroll courses
- iii. Sign attendance with captured unique (picture and) fingerprint biodata
- iv. Track sign-in and attendance percentage

C. Attendance Management

- i. Record students registration and course enrolment data
- ii. Records of students absent and present days per course
- iii. Records of login time and attendance percentage per course
- iv. Records of promptness (with respect to class start time, estimated time to take all class attendance and students sign-in time)
- v. Records of lecturer sign-in time and class start time
- vi. Records of all courses and attendance data

D. Security

- i. Takes attendance with unique fingerprint data
- ii. Allows only one sign-in per class for students
- iii. Attendance for a class (day) can be taken only in that day (no falsified attendance)
- iv. Only a lecturer of a course can start attendance sign-in process
- v. No student can register more than once
- vi. Attendance can be taken via fingerprint scanner
- vii. Report unregistered persons in the database

Development of Process diagram for Fingerprint Attendance Tracking System

The recording steps to register a new User, record attendance, and generate attendance reports are described below. The process flow diagram is as shown in Figure 6. The processes and cases used to describe Fingerprint Attendance Tracking System are as follows:

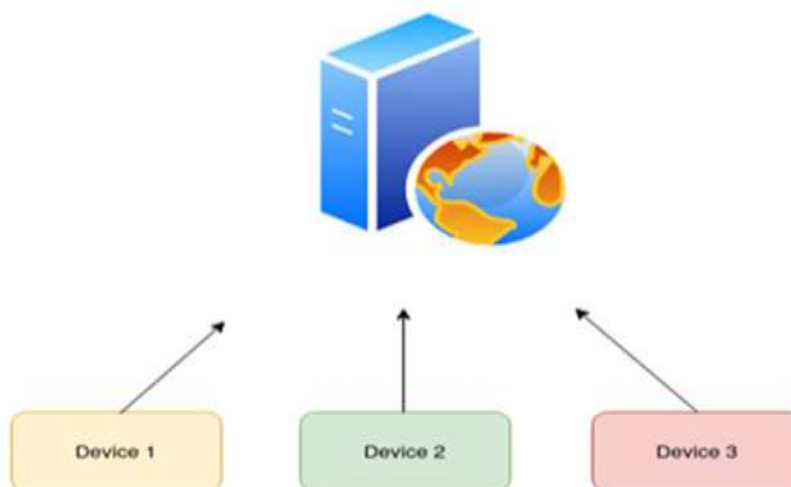


Figure 6: Biometric Attendance System Architecture

Register a New User

Primary Actor: System Administrator

Goal: To add a new user's fingerprint to the system database.

Preconditions: Administrator is authenticated and has access to the system.

Main Steps:

1. Administrator logs into the system.
2. Selects the option to add a new user.
3. Enters user details (name, ID, etc.).
4. User places his/her finger on the fingerprint sensor.
5. System captures and processes the fingerprint.
6. System stores the fingerprint template in the database.
7. Confirmation message displayed to administrator.

Post-conditions: User's fingerprint is stored and ready for attendance tracking.

Extensions:

- 4a. If fingerprint capture fails, prompt user to retry.
- 6a. If the database is unreachable, display an error and retry the operation.

Record Attendance

Primary Actor: User (Student)

Goal: To record the user's attendance through fingerprint verification.

Preconditions: User's fingerprint is already registered in the system.

Main Steps:

1. User places their finger on the fingerprint sensor.
2. System captures the fingerprint and processes it.
3. System compares the fingerprint with stored templates.
4. If a match is found, record the attendance time and date.
5. System displays a success message on the screen.

Post-conditions: Attendance is recorded in the system.

Extensions:

- 3a. If no match is found, display a "No Match Found" message and prompt for a retry.

Generate Attendance Reports

Primary Actor: System Administrator

Goal: To generate reports based on recorded attendance data.

Preconditions: Administrator is authenticated and has access to the system.

Main Steps:

1. Administrator logs into the system.
2. Selects the option to generate attendance reports.
3. Chooses the report criteria (date range, user, etc.).
4. System queries the database and generates the report.
5. System displays or exports the generated report.

Post-conditions: Administrator obtains the desired attendance report.

Extensions:

- 4a. If no data is available for the selected criteria, display a "No Data" message.

RESULTS AND DISCUSSION

The findings of "Development of an ESP32-Microcontroller-Based Biometric System for Classroom Management", highlighting the key results obtained from the data analysis. The discussion section provides an interpretation of these results exploring their implications, limitations and correlations with existing literature. The findings are organized in three sections, each addressing a specific research objective.

Development of real-time-system module

The development of a real-time-system module that captures individual (Student and Lecturer) bio-data (fingerprint) and generate reports is systematically documented.

Figure 7 is a picture of the prototype as assembled by the researcher. The breadboard housing the ESP32 microcontroller and other components, including the jumper cables are neatly packaged in the plastic box.



Figure 7: Picture of assembled prototype attendance device

Attendance List Module

The Attendance List Module provides a real-time, comprehensive view of attendance data recorded by the fingerprint attendance system. It allows administrators and authorized personnel to monitor, analyze, and manage attendance records effectively. This module is integral for ensuring accuracy in attendance tracking and for facilitating easy access to attendance information. Figure 8 shows the Attendance list module

ID	NAME	MATRIC NUMBER	FINGERPRINT ID	DEVICE DEP.	DATE	TIME IN	TIME OUT
2	Eng	0	36	Enrollment	2024-05-09	17:43:14	17:47:26
1	Ken Eboh	0	36	Enrollment	2024-05-09	16:48:37	16:48:38

Figure 8: Attendance List Module

Changing Device Module

The Changing Device Module is an important aspect of the Fingerprint Attendance Tracking System, particularly in managing and switching between different operational modes such as enrollment and attendance tracking. This module enhances the system's

flexibility and usability by allowing administrators to adapt the device settings according to specific requirements. Figure 9 shows the changing device module.

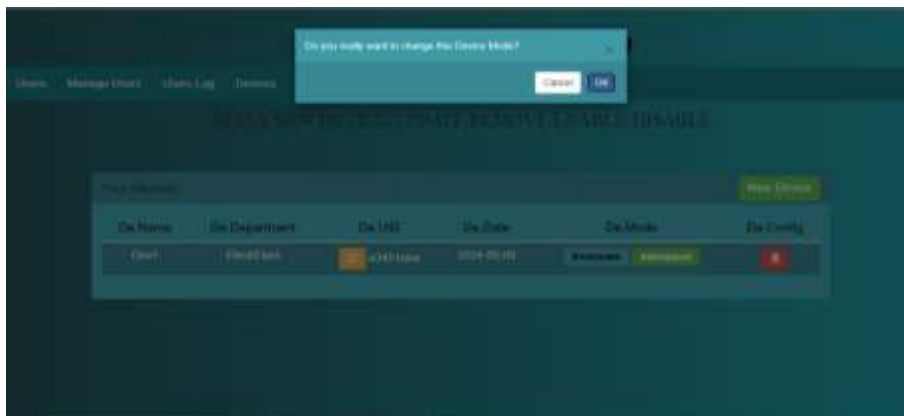


Figure 9: The Changing Device Module

Deleted User Module

The Deleted User Module is a vital component of the Fingerprint Attendance Tracking System, designed to manage and maintain records of users who have been removed from the system. This functionality is crucial for maintaining data integrity, ensuring compliance with data retention policies, and facilitating audits or reviews if necessary. Figure 10 shows the deleted user module.

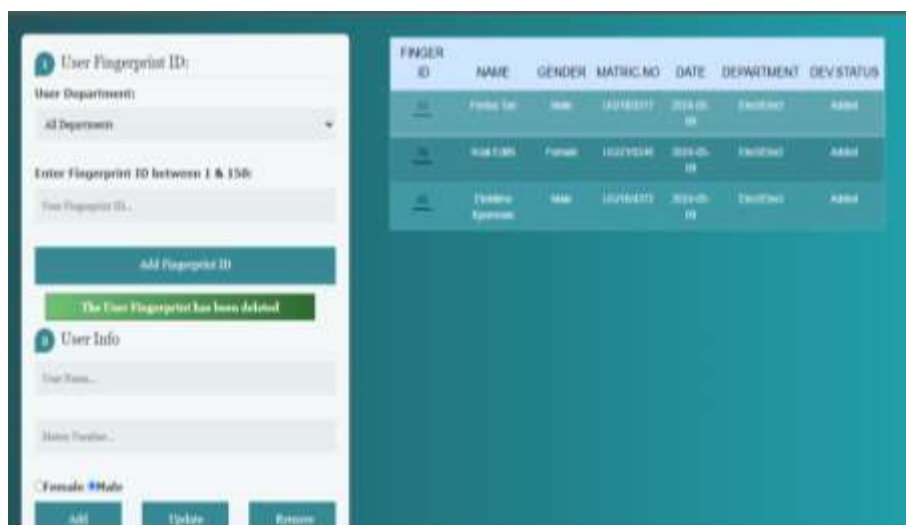


Figure 10: Deleted User Module

User Log Module

The user log module is developed for lecturer to log in to generate attendance report. The User Log Module, particularly focused on generating reports and exporting data to Excel, is a vital component of the Fingerprint Attendance Tracking System. This module plays a crucial role in data analysis, decision-making, and maintaining records for compliance and review purposes. Figure 11 shows the user log module.



Figure 11 User Log Module

Updating Enrolled Student Information Module

The Updating Enrolled Student Information Module is a critical component of the Fingerprint Attendance Tracking System, especially in educational settings where student details may frequently change due to new academic years, course changes, or personal information updates. This module ensures that the system maintains accurate and current records of all enrolled students. Figure 12 shows the updating Enrolled Student Information Module

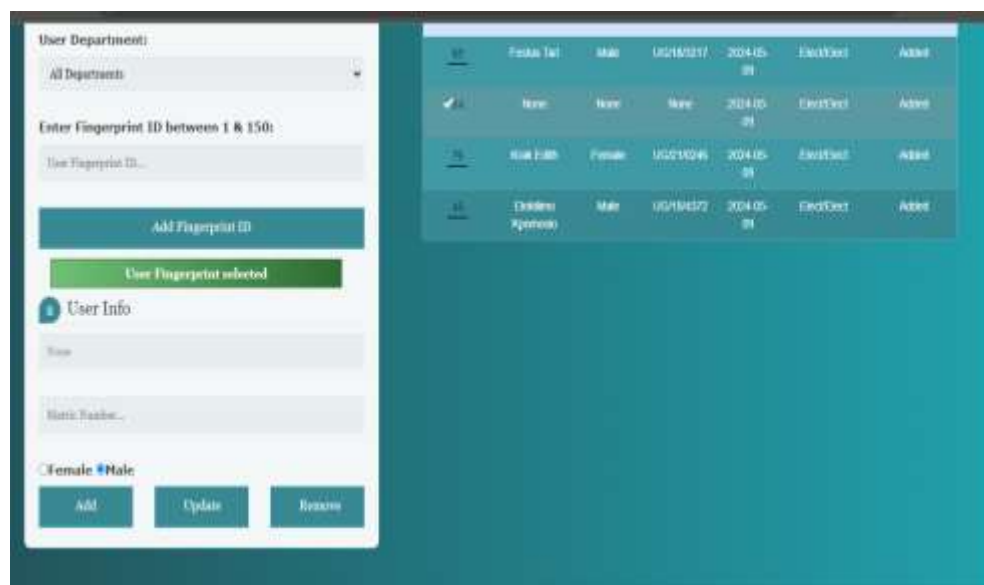


Figure 12 Updating Enrolled Student Information Module

User Enrolment and Data Acquisition

Prior to the deployment of the device, the users of the system (lecturers and students) are required to furnish relevant information to the System Administration Office with relevant data for upload. This is very important to ease the stress of enrolling users in the classroom. Note: 1234 is used as the passcode for all lecturers. After users have been successfully added to the database, they can enroll using the ESP32 Device and the Fingerprint Scanner to verify. A total of one hundred and sixty-three (163) users – (one hundred and forty-three final year Electrical Engineering students and twenty-one lecturers' details from the department) were uploaded. A total of forty-seven courses were uploaded and assigned to lecturers as well. The data capture in Figure 13 is used to provide relevant information.

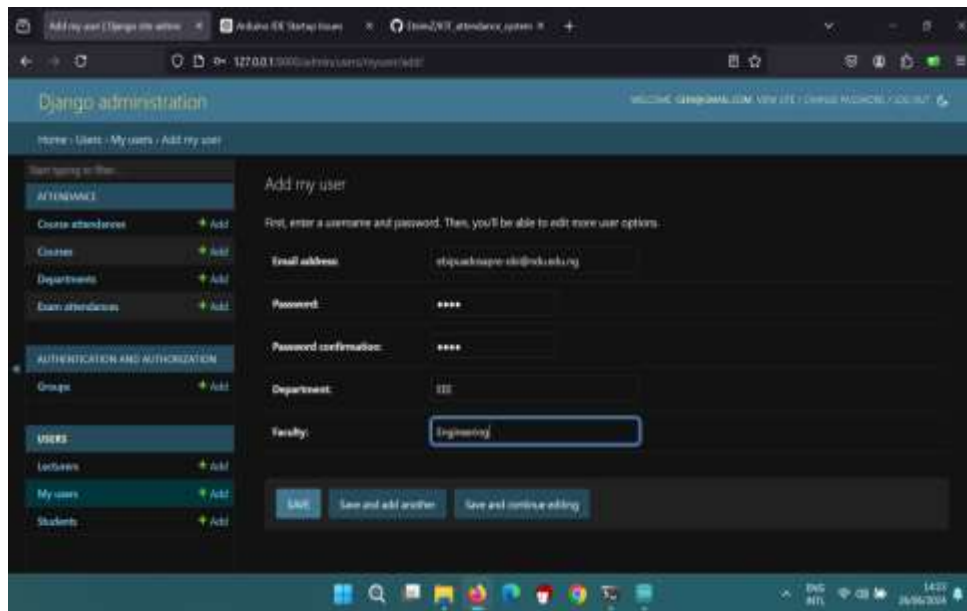


Figure 13: Screen Capture for User addition

Electronic attendance sheet for Courses showing percentage attendance

To test and validate the performance of the proposed fingerprint-based attendance system, students from the department registered their fingerprints on the system for three different courses. The selected courses for this analysis were EEE 564 (Antenna and Propagation), EEE 555 (Electronic System Design), and EEE 531 (Microprocessor Applications).

The results of the system are displayed in several tables. Table 1 focuses on the attendance data for EEE 531. This table provides a comprehensive overview of student attendance over twelve class sessions. From the data in Table 1, it is evident that attendance varied significantly among the students. To further validate the system's effectiveness, the attendance for EEE 555 was also recorded and analyzed, as shown in Table 2. This table provides a comprehensive overview of student attendance over ten class sessions. These varied attendance rates highlight the system's capability to accurately track and record attendance across multiple sessions and courses.

Table 1: Attendance Register for EEE 531

	07/07/2025	14/07/2025	21/07/2025	28/07/2025	04/08/2025	11/08/2025	18/08/2025	25/08/2025	01/09/2025	08/09/2025	15/09/2025	22/09/2025	% ATTENDANCE
Student													
test student - 0000	X	X	X	X	X	X	X	X	X	X	X	X	0.00
AJOKO TAMARALAYEFA GABRIELLA - 190714	1	1	1	1	1	1	1	1	1	1	1	1	100.00
ANUBIRI SOLOMON CHINEDU - 190720	X	X	X	1	1	1	X	X	1	X	X	1	41.60
BURABARI BARIDAM - 190723	1	X	X	1	1	1	1	X	1	X	X	1	58.33
EGBERIBIN AYIBAMIEBI - 190725	X	1	1	1	1	1	X	X	1	1	1	X	66.66
EMEKA VICTOR CHIGOZIE - 190726	1	X	X	X	1	1	1	1	X	X	1	1	58.33

GBOUN MARVELLOUS EMMANUEL - 190730	X	1	1	1	1	X	1	1	1	1	1	1	83.33
OKPAKO OGHENETEGA - 190742	1	X	X	1	1	1	1	X	1	X	X	1	58.33
ORJI EMMANUEL CHINONSO - 190745	1	1	1	X	1	1	1	X	1	1	1	1	83.33
ORUAMA GODDOWELL - 190746	1	1	1	X	1	1	X	1	1	X	X	X	58.33
FEKOWEIMO ALAOWEI - 192316	1	X	X	X	1	1	1	1	1	X	1	1	66.66
IYORO EBITARE JOSEPH - 192321	X	X	X	1	1	1	1	1	1	X	1	1	66.66
WILCOX LEMMY RICHARD - 193011	1	1	1	1	1	1	1	1	X	X	1	X	75.00
BROWN GOBARI JASPER - 193600	X	X	X	X	X	1	1	1	1	X	1	1	50.00
IDOWU OLAMILEKAN JOSEPH - 193605	X	1	1	1	1	1	1	1	1	1	1	1	91.66
FELIX FABOPREGHE DENIS - 194355	X	X	X	1	1	1	1	1	1	X	X	1	58.33
ORUKARI RICHARD EBINIPRE - 194535	X	X	X	1	X	1	1	1	1	X	1	X	50.00
MICHAEL ADVICE OTU - 95344587	X	X	X	1	1	1	X	1	1	X	X	1	50.00
ISAIAH INNOCENT - 97333833	X	X	X	1	1	1	1	X	1	X	1	1	58.33

Table 2: Attendance Register for EEE 555

Student	02/07/2025	09/07/2025	09/07/2025	16/07/2025	23/07/2025	30/07/2025	06/08/2025	13/08/2025	20/08/2025	27/08/2025	% ATTENDANCE
test student - 0000	X	X	X	X	X	X	X	X	X	X	0
AJOKO TAMARALAYEFA GABRIELLA - 190714	1	1	1	1	1	1	1	1	1	1	100
ANUBIRI SOLOMON CHINEDU - 190720	X	X	X	1	1	1	X	X	1	X	40
BURABARI BARIDAM - 190723	1	X	X	1	1	1	1	X	1	X	60
EGBERIBIN AYIBAMIEBI - 190725	X	1	1	1	1	1	X	X	1	1	70
EMEKA VICTOR CHIGOZIE - 190726	1	X	X	X	1	1	1	1	X	X	50
GBOUN MARVELLOUS EMMANUEL - 190730	X	1	1	1	1	X	1	1	1	1	80
OKPAKO OGHENETEGA - 190742	1	X	X	1	1	1	1	X	1	X	60
ORJI EMMANUEL CHINONSO - 190745	1	1	1	X	1	1	1	X	1	1	80
ORUAMA GODDOWELL - 190746	1	1	1	X	1	1	X	1	1	X	70
FEKOWEIMO ALAOWEI - 192316	1	X	X	X	1	1	1	1	1	X	60
IYORO EBITARE JOSEPH - 192321	X	X	X	1	1	1	1	1	1	X	60
WILCOX LEMMY RICHARD - 193011	1	1	1	1	1	1	1	1	X	X	80
BROWN GOBARI JASPER - 193600	X	X	X	X	X	1	1	1	1	X	40
IDOWU OLAMILEKAN JOSEPH - 193605	X	1	1	1	1	1	1	1	1	1	90
FELIX FABOPREGHE DENIS - 194355	X	X	X	1	1	1	1	1	1	X	60
ORUKARI RICHARD EBINIPRE - 194535	X	X	X	1	X	1	1	1	1	X	50

MICHAEL ADVICE OTU - 95344587	X	X	X	1	1	1	X	1	1	X	50
ISAIAH INNOCENT - 97333833	X	X	X	1	1	1	1	X	1	X	50

Table 3 is the attendance record of students for Electronics Systems Design (EEE 555), over eleven (11) class sessions. The data in the table implies that the course lecturer taught only eleven times in the semester. Hence the percentage attendance is a function of the number of times a course lecturer was in class and actually started and ended the course. These results show 100% performance of the current system, though tested for a very short period. It is interesting to note that attendance records can neither be manipulated by students nor the academics.

CONCLUSION AND RECOMMENDATIONS

Conclusion

Attendance management is a critical aspect of administrative operations in higher institutions. Traditional methods of recording attendance, such as manual entry in registers or signing attendance sheets, are often fraught with issues like time consumption, inaccuracies, and the potential for manipulation or fraud. These methods can be labour-intensive and error-prone, leading to challenges in maintaining accurate attendance records. In recent years, technological advancements have paved the way for more efficient and reliable attendance management systems. Biometric technology, which uses unique physical characteristics for identification, has emerged as a promising solution. Among various biometric methods, fingerprint recognition is widely regarded as one of the most secure and convenient options due to the uniqueness and permanence of fingerprints.

The development and implementation of a microcontroller-based biometric (fingerprint) attendance and management system for higher institutions present a significant advancement in the field of educational administration. After rigorous tests, the results show that: - Image acquisition time: 0.5 seconds, - False Acceptance Rate (FAR): 0.2%, and - False Rejection Rate (FRR): 0.5%. The system demonstrated high accuracy and efficiency, with rapid image acquisition and low error rates. The FAR and FRR results indicate a high level of security and reliability, ensuring that only registered students can access the classroom and that legitimate students are not denied access.

This system offers numerous benefits, including: improved attendance accuracy and reduced fraud, Reduced administrative burdens and increased efficiency, and Real-time insights into students and lecturers' attendance patterns. By harnessing the power of biometric technology and IoT connectivity, this system has the potential to revolutionize attendance tracking and classroom management in educational institutions. Its scalability, ease of use, and cost-effectiveness make it an attractive solution for schools and universities seeking to modernize their attendance and administrative processes. Due to the unique nature of fingerprints, it was practically impossible to impersonate during examinations and falsify attendance records. This study provides a foundation for further research and development in this area, including the integration of additional functionalities and the exploration of other biometric modalities like the iris, taking care of the physically challenged.

This work has demonstrated that leveraging fingerprint recognition technology can greatly enhance the accuracy, efficiency, and security of attendance management processes. The traditional methods of attendance recording, plagued by inaccuracies, time consumption, and potential for fraud, are effectively addressed by the proposed biometric system. By integrating a fingerprint sensor with a microcontroller, the system ensures that only authenticated individuals can record their attendance, thereby eliminating the possibility of proxy attendance and other fraudulent practices.

The dissertation has outlined the design, implementation, and testing of the biometric attendance system. The hardware and software components were carefully selected and integrated to create a cohesive system that meets the specific needs of higher institutions. The system's performance was thoroughly tested, and the results indicated a high level of accuracy and reliability in capturing and managing attendance data. Moreover, the biometric attendance system offers several additional benefits, including real-time data access, automated record-keeping, and the ability to generate detailed attendance reports. These features not only streamline administrative tasks but also provide valuable insights into attendance patterns and trends, which can inform decision-making and improve overall institutional management. Despite the initial challenges related to cost, technical expertise, and privacy concerns, the long-term benefits of the biometric system are evident. The investment in such technology is justified by the substantial improvements in attendance management and the associated administrative efficiencies.

A microcontroller-based biometric attendance system leverages fingerprint recognition technology to automate and streamline the process of recording attendance. By integrating fingerprint sensors with microcontrollers, such systems can accurately and efficiently capture, store, and manage attendance data. This reduces the burden on administrative staff and minimizes the risk of errors and fraudulent activities. The microcontroller-based biometric (fingerprint) attendance and management system represents a significant step forward in modernizing attendance management in higher institutions. Its successful implementation has the potential to transform traditional practices, offering a more secure, efficient, and accurate solution that benefits both administrators and students.

- i. Traditional methods of recording attendance, such as manual entry in registers or signing attendance sheets, are often fraught with issues like time consumption, inaccuracies, and the potential for manipulation or fraud.

- ii. Among various biometric methods, fingerprint recognition is widely regarded as one of the most secure and convenient options due to the uniqueness and permanence of fingerprints
- iii. The development and implementation of a microcontroller-based biometric (fingerprint) attendance and management system for higher institutions present a significant advancement in the field of educational administration.
- iv. This study has demonstrated that leveraging fingerprint recognition technology can greatly enhance the accuracy, efficiency, and security of attendance management processes.
- v. The results have shown that the system is reliable, cost-effective, reliable, flexible and error-free.

Recommendations

Future work in this area could focus on expanding the system's capabilities, such as integrating it with other institutional management systems, enhancing data security measures, and exploring the use of other biometric modalities. Additionally, conducting pilot studies in various higher institutions would provide further insights into the system's adaptability and effectiveness in different contexts.

The following are recommendations for further research:

1. To create a more robust system, the Raspberry Pi MCU should be used in the design due to its flexibility, expandable memory and speed, despite being significantly more expensive.
2. Implement a combination of fingerprint and iris recognition, as both biometric parameters have unique features that are specific to individuals. A combination of the two bio-data of individuals will significantly increase the security features and become more adaptable to a wider audience and variety of applications.
3. An integration of image processing will significantly reduce the time taken to capture attendance (though with a very high memory/storage requirement).
4. Collaborative efforts should be undertaken to ensure the system's comprehensive development and integration.
5. In very large organisations with delivery and quality requirements, video cameras may be installed in strategic areas (classrooms in the case of higher institutions), covering blind spots and ensuring compliance.

REFERENCES

- Ahsan, Q. (2006). Compact information technology enabled systems for intelligent process monitoring. Cardiff University (United Kingdom).
- Bhanu, B., & Chen, H. (2008). Human ear recognition by computer. Springer Science & Business Media.
- Budiarto, M., Audiah, S., Astuti, E. D., Sanjaya, Y. P. A., & Firli, M. Z. (2024, August). Enhancing School and College Attendance Using Advanced Technology. In 2024 3rd International Conference on Creative Communication and Innovative Technology (ICCIIT) (pp. 1-6). IEEE.
- Delac, K., & Grgic, M. (2004, June). A survey of biometric recognition methods. In Proceedings. Elmar-2004. 46th International Symposium on Electronics in Marine (pp. 184-193). IEEE.
- Dong, W., Li, B., Guan, G., Cheng, Z., Zhang, J., & Gao, Y. (2020). TinyLink: A holistic system for rapid development of IoT applications. *ACM Transactions on Sensor Networks (TOSN)*, 17(1), 1-29.
- Gadade, B., Mulani, A. O., & Harale, A. D. (2024). IOT Based Smart School Bus and Student Monitoring System. *NATURALISTA CAMPANO*, 28(1), 730-737.
- Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). Handbook of fingerprint recognition (Vol. 2). London: springer.
- Mehrotra, H., Bours, P., & Venkatesh, S. (2021). A review of continuous authentication using behavioral biometrics on mobile devices. *Pattern Recognition*, 122, 108170. - includes accuracy metrics for different biometric modalities including fingerprint.
- Moses, K. R., Higgins, P., McCabe, M., Prabhakar, S., & Swann, S. (2011). Automated fingerprint identification system (AFIS). The fingerprint sourcebook, 1, 1-6.
- Oloyede, M. O., Hancke, G. P., & Myburgh, H. C. (2020). A review on face recognition systems: recent approaches and challenges. *Multimedia Tools and Applications*, 79(37), 27891-27922.
- Pugliese, A. J. (2016). Biometrics: improving authentication in information systems. *The CPA Journal*, 86(3), 69. - established need for biometric solutions to replace manual authentication methods.
- Scott, J. (2015). Body Markers: Attendance Tracking Devices and Presentism Control. *Contemporary Readings in Law & Social Justice*, 7(2).
- Shoewu, O., & Idowu, O. A. (2012). Development of attendance management system using biometrics. *The Pacific Journal of Science and Technology*, 13(1), 300-307.
- Tarmissi, K., Allaaboun, H., Abouellil, O., Alharbi, S., & Soqati, M. (2024, January). Automated Attendance Taking System using Face Recognition. In 2024 21st Learning and Technology Conference (L&T) (pp. 19-24). IEEE.
- Yeap, K. H., Chow, C. T., Low, H. T., & Nisar, H. (2024). Enhanced Biometric Identification Using Photoplethysmography Signals. Cambridge Scholars Publishing.